BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-202

30 AUGUST 2001

Communications and Information

COMPUTER SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://afpubs.hq.af.mil.**

OPR: HQ AFCA/GCI (MSgt Gorom)

Certified by: HQ USAF/SCXX (Mr. James J. Hundley

Supersedes AFI 33-202, 15 February 2001

Pages: 84

Distribution: F

This instruction implements the computer security (COMPUSEC) portion of Air Force Policy Directive (AFPD) 33-2, *Information Protection*, (will become Information Assurance) and establishes Air Force COMPUSEC requirements for information protection to comply with Public Law (P.L.) 100-235, *Computer Security Act of 1987*; Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*; OMB Bulletin 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*; Department of Defense Directive (DoDD) 5200.28, *Security Requirements for Automated Information Systems (AIS)*, March 21, 1988; DoDI 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*, December 30, 1997; and Department of Defense (DoD) 8510.1-M, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, July 31, 2000. The Uniform Code of Military Justice applies to personnel who violate the specific prohibitions and requirements of this instruction. You may use extracts from this Air Force instruction (AFI). Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/ITPP), 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/GCI, 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222, and HQ USAF/SCMI, 1250 Air Force Pentagon, Washington DC 20330-1250. Send supplements to this publication to HQ AFCA/GCI for review, coordination, and approval prior to publication. For a glossary of references and supporting information refer to **Attachment 1** and AFDIR 33-303, *Compendium of Communications and Information Technology*. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF REVISIONS

This change updates IC 2000-1 (**Attachment 4**) and IC 2001-1 (**Attachment 5**). It includes reference to an additional DoD instruction and manual. Updates and clarifies policy for foreign national access. Adds a statement that personally owned information systems will be confiscated if contaminated with classified

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
30 Aug 2001	N/A	-

Title and Subtitle Air Force Instruction 33-202, Communications and Information Computer Security	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Secretary of the Air Force Pentagon Washington, DC 20330-1250	**Performing Organization Report Number** AFI33-202
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 84	

information. Adds policy on wireless local area network (WLAN) and additional requirements for PDA usage, including an example of a PDA usage statement (**Attachment 3**). Adds **Chapter 4**, which talks about the certification and accreditation (C&A) process. References to AFSSI 5024 were changed to reflect this document and the term Computer System Security Officer is changed to Information System Security Officer (ISSO). Adds a new attachment (**Attachment 2**) that lists the C&A tasks. Updates the title to AFSSI 5021 and changes AFCERT Advisories to Time Compliance Network Order (TCNO). Updates assignment of the Designated Approving Authority (DAA). Updates the training requirements for users and unit COMPUSEC managers and references, abbreviations and acronyms, and terms. See the last attachment of this publication (**Attachment 6**, IC 2001-2) for the complete IC. A "|" indicates revised material since the last edition.

Chapter 1

GENERAL INFORMATION

1.1. Purpose. This instruction gives the directive requirements for the COMPUSEC component of the information assurance (IA) discipline as outlined in AFPD 33-2 and implements the Air Force COMPUSEC Program. This instruction applies to all Air Force military and civilian personnel and to Air Force contractors who develop, acquire, deliver, use, operate, or manage Air Force information systems.

1.2. Introduction. COMPUSEC is one of the IA disciplines promulgated in AFPD 33-2. Compliance assures measures are taken to protect all Air Force information system resources and information effectively and efficiently. Appropriate levels of protection against threats and vulnerabilities for information systems prevent denial of service, corruption, compromise, fraud, waste, and abuse.

1.3. Applicability. More restrictive DoDD and Director of Central Intelligence Agency directive requirements governing Special Category information or Special Access Program information take precedence over this.

1.4. Objectives. The objectives of COMPUSEC are to protect and maintain the availability, integrity, confidentiality, and accountability of information system resources and information processed throughout the system's life cycle. (**NOTE:** Authenticity and nonrepudiation are security services achieved by implementing accountability.) Use countermeasures to achieve the four objectives. Each safeguard and its associated control constitute a countermeasure. Security disciplines such as COMPUSEC, information security, emissions security, communications security (COMSEC), etc., provide safeguards to protect information. Controls are those administrative and management activities that implement the safeguards.

1.5. DELETED.

1.5.1. DELETED.

1.5.1.1. DELETED.

1.5.1.2. DELETED.

1.5.1.3. DELETED.

1.5.2. DELETED.

1.5.3. DELETED.

1.5.3.1. DELETED.

1.5.3.2. DELETED.

1.5.3.3. DELETED.

1.5.3.4. DELETED.

1.5.4. DELETED.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Headquarters United States Air Force Deputy Chief of Staff for Communications and Information (HQ USAF/SC). HQ USAF/SC manages the Air Force COMPUSEC Program.

2.2. Headquarters Air Force Communications Agency.

2.2.1. Reviews, evaluates, and interprets national and DoD COMPUSEC policy and doctrine, and makes recommendations on implementation to HQ USAF/SCM.

2.2.2. Develops, coordinates, and maintains HQ USAF/SC-approved Air Force COMPUSEC instructions, manuals, and pamphlets.

2.2.3. Develops, coordinates, publishes, and maintains HQ USAF/SCM-coordinated specialized COMPUSEC publications.

2.2.4. Provides guidance and support to MAJCOMs, field operating agencies (FOA), and direct reporting units (DRU) in developing, implementing, and managing their COMPUSEC programs.

2.2.5. Manages the process of assessing government-produced and commercial-off-the-shelf software and hardware subsystem security features.

2.2.6. Develops security techniques and procedures with Air Force-wide applicability, coordinates the information with HQ USAF/SCM, and distributes this information to MAJCOMs.

2.2.7. Processes waiver or deviation requests to Air Force COMPUSEC policy and instructions.

2.3. Headquarters Air Intelligence Agency (HQ AIA). Provides guidance concerning security requirements and implementation of information systems in Sensitive Compartmented Information facilities.

2.4. Air Force Information Warfare Center (AFIWC).

2.4.1. Collects and analyzes technical vulnerability information. Develops countermeasures or requests assistance from appropriate agencies. Advises Air Force users on appropriate countermeasures.

2.4.2. Obtains and distributes IA threat and vulnerability information to appropriate users.

2.4.3. Assists Air Force organizations in evaluating information systems security, recommending IA countermeasures, developing IA requirements documents, and advocating funding for IA research and development programs.

2.4.4. Maintains a database of COMPUSEC information reported by Air Force organizations and sends copies of the reports to all affected Air Force organizations.

2.5. Headquarters Air Force Materiel Command (HQ AFMC).

2.5.1. Assists HQ AFCA in developing COMPUSEC guidance and procedures for information systems in the acquisition and development life cycle.

2.5.2. Establishes IA training for single managers.

2.5.3. The Single Manager:

2.5.3.1. Ensures information systems they acquire and develop comply with COMPUSEC policies.

2.5.3.2. Develops a certification and accreditation (C&A) plan and documents it in the System Security Authorization Agreement (SSAA).

2.5.3.3. Certifies and accredits information systems according to **Chapter 4** of this AFI and performs duties identified for the Program Manager.

2.5.3.4. Continuously identifies and analyzes threats and vulnerabilities to the information system and its information to maintain an appropriate level of protection.

2.5.3.5. Ensures design reviews address information system security requirements.

2.5.3.6. Establishes security controls that protect the information system during development.

2.5.3.7. Ensures information system life-cycle responsibilities are documented. This includes responsibility for reaccomplishing risk analysis, security testing, and certification due to modifications or changes to the system.

2.5.3.8. Ensures operating agencies receive copies of the SSAA documentation.

2.5.3.9. Ensures the SSAA documentation defines security procedures for system users, administrators, and maintainers.

2.5.3.10. Addresses all security-related issues to the systems security working group (see AFI 31-702, *System Security Engineering*).

2.5.3.11. Determines the sensitivity level of the information and the criticality of information system resources and information.

2.5.3.12. Plans and programs budgetary, manpower, and training support for the implementation and continuation of the COMPUSEC program to include improvements to security.

2.5.3.13. Ensures the Designated Approving Authority (DAA) and users participate throughout the system development cycle in security analyses performed in conjunction with all design and specification reviews.

2.5.3.14. Is responsible for ensuring the appropriate coordination and review of all decisions concerning security trade-off and changes in requirements with the Certifier, system developers, users, and the DAA (see AFI 31-702).

2.5.3.15. Is the focal point for security system engineering during the system requirements definition, design, implementation, and testing phases of the program.

2.5.3.16. Responsible for ensuring security measures are implemented to adequately satisfy the security specification and any residual risks are identified.

2.6. Other Agencies Acquiring or Developing Information Systems or Software. Assume single manager responsibilities (paragraph **2.5.3.**) when they develop systems or software outside a program management office structure.

2.7. Designated Approving Authority:

2.7.1. Allocates funding and manpower resources to achieve and maintain an appropriate level of protection and to remedy security deficiencies.

2.7.2. As necessary, appoints a DAA representative to deal with the day-to-day issues of accrediting information systems according to **Chapter 4**.

2.7.3. Identifies Information Systems Security Officers (ISSO) for all information systems under the DAA's jurisdiction.

2.7.4. Ensures IA personnel review all information system requirements documents to ensure IA requirements are appropriately addressed.

2.7.5. Appoints a certifier to accomplish information system certification. Makes sure this individual possesses the technical expertise on the information system being certified and on the security mechanisms in use.

2.7.6. Makes appropriate decisions to balance security requirements, mission, and resources against the defined or perceived threat.

2.7.7. Ensures resources are available to support the certification and security countermeasures.

2.7.8. Formally assumes responsibility for the secure operation of the information system to operate in a specific environment.

2.7.9. Ensures the security policy is developed and certification goals are clearly defined.

2.7.10. Is responsible for approving security requirements documents, memorandums of agreement, and deviations from security policy.

2.7.11. Accredits all information systems and applications under their authority prior to their operation.

2.8. Certifier:

2.8.1. Coordinates certification activities and places all documentation into the SSAA for presentation to the DAA.

2.8.2. Leads certification teams formed to certify complex or large networks.

2.8.3. Based on system certification, makes technical judgments of an information system's compliance with the systems security policy, and develops an accreditation recommendation for submission to the DAA.

2.8.4. Is the formal certifying authority for the system and ensures the SSAA appropriately addresses the system security policy objectives.

2.8.5. Validates and assesses the risks associated with operating the system.

2.9. Major Commands. MAJCOMs implement and manage a COMPUSEC program throughout the command. FOAs and DRUs that elect to manage their own programs must document that in a support agreement according to AFI 25-201, *Support Agreements Procedures*.

2.9.1. MAJCOM IA Office. Implements and oversees the MAJCOM COMPUSEC program.

2.9.1.1. Sends copies of any command supplements to Air Force COMPUSEC instructions and policies to HQ AFCA/GCI and HQ AFCA/XPXP.

2.9.1.2. Assists subordinate units in developing their COMPUSEC programs.

2.9.1.3. Ensures communications and information system requirements documents include appropriate COMPUSEC requirements.

2.9.1.4. Reviews audit, vulnerability, and security survey reports for applicability within the command. Implements measures to correct deficiencies.

2.9.1.5. DELETED.

2.9.1.6. Ensures controls are in place to collect information system accreditation metric data according to AFI 33-205, *Information Protection Metrics and Measurements Program*.

2.9.1.7. Designates a focal point to track and ensure MAJCOM compliance with C&A requirements for both classified and unclassified systems. The MAJCOM focal point acts as the point of contact (POC) to the Defense Information Systems Agency (DISA) for the command regarding the SSAA documentation.

2.10. Wings. Establish a base-wide COMPUSEC program administered by the wing IA office. Obtain assistance and guidance from the wing IA office for IA requirements, technical solutions, and implementation.

2.10.1. Wing IA Office:

2.10.1.1. Assists the wing communications and information systems officer (CSO) and all base organizations and tenants in the development and management of their COMPUSEC programs.

2.10.1.2. Designates a single focal point to track and ensure wing and tenant unit compliance with C&A requirements for both classified and unclassified information systems. Identifies non-compliant systems and get-well dates. Provides information to local network control center (NCC) and MAJCOM IA office.

2.10.1.3. Routinely verifies with the NCC that only accredited systems (classified and unclassified) are connected to the base network.

2.10.1.4. Provides accreditation guidance and assistance.

2.10.1.5. Ensures information system requirements documents include appropriate COMPUSEC requirements.

2.10.1.6. Sends copies of any base supplements to Air Force COMPUSEC instructions and policies to their respective MAJCOMs.

2.10.1.7. DELETED.

2.10.2. NCC. The NCC manages the local infrastructure that provides customers the communications and information resources needed to achieve their operational objectives. Consult AFI 33-115V1, *Network Management*, and AFSSI 5027, *Network Security Policy*, for detailed descriptions of the IA roles performed at the NCC by network managers, information protection operators, system administrators, help desk technicians, and workgroup managers.

2.11. Organizations. Commanders appoint in writing a unit COMPUSEC manager to oversee their COMPUSEC program. Unless required by the MAJCOM or wing, official designation of ISSOs is at the discretion of the unit COMPUSEC manager. If the ISSO positions are not assigned, the ISSO responsibilities reside with the unit COMPUSEC manager.

2.11.1. Unit COMPUSEC Manager:

2.11.1.1. Implements a unit COMPUSEC program to ensure compliance with the provisions of this instruction, including any MAJCOM or wing supplements.

2.11.1.2. Is the single liaison between the unit and the wing IA office for COMPUSEC matters.

2.11.1.3. Ensures all users and IA personnel receive training.

2.11.1.4. Provides a copy of appointment letter to the wing IA office.

2.11.1.5. Ensures ISSOs are assigned to functional systems or on a system-by-system basis.

2.11.1.6. Provides C&A information to the wing IA office for appropriate tracking.

2.11.2. DELETED.

2.11.2.1. DELETED.

2.11.2.2. DELETED.

2.11.2.3. DELETED.

2.11.2.4. DELETED.

2.11.2.5. DELETED.

2.11.2.6. DELETED.

2.11.2.7. DELETED.

2.11.2.8. DELETED.

2.11.2.9. DELETED.

2.11.2.10. DELETED.

2.11.3. ISSO. Workgroup managers (WM) may perform some or all of the duties listed below:

2.11.3.1. Establishes controls to ensure users operate, maintain, and dispose of information systems according to existing policy and procedures, including the system security policy.

2.11.3.2. Ensures procedures are in place for users to notify the ISSO or alternate if problems arise during critical or classified processing.

2.11.3.3. Ensures the system security policy for each information system is distributed to system users.

2.11.3.4. Establishes controls that ensure audit trails are periodically reviewed.

2.11.3.5. Performs an initial evaluation of each vulnerability or incident and begins corrective or protective measures and reports according to AFSSI 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting* (will become AFMAN 33-225, Volumes 1 and 2).

2.11.3.6. Evaluates known vulnerabilities to ascertain if additional safeguards are needed to protect information systems.

2.11.3.7. Ensures all network and system administrators are taking aggressive action to implement TCNO and comply with the vulnerability and incident reporting procedures according to AFSSI 5021 (will become AFMAN 33-225, Volumes 1 and 2).

2.11.3.8. Ensures users receive training on system-specific security procedures, and informs network and system administrators to frequently check vendor sources for information regarding vulnerabilities for their particular hardware and software.

2.11.3.9. Periodically validates user-access privilege levels.

2.11.3.10. Maintains the accreditation according to **Chapter 4**.

2.11.3.11. DELETED.

2.11.3.12. Ensures organizations do not use shareware or public domain software until approved for use by the DAA. The ISSO ensures the software is free of viruses, hidden defects, and obvious copyright infringements. The ISSO or WM perform testing.

2.11.3.13. Monitors information system activities to ensure system integrity; establishes reaction and maintenance controls for the facility; and performs system access or revocation tasks.

2.11.3.14. Continually identifies threats, deficiencies, and associated countermeasures.

2.11.3.15. Reports system security incidents, vulnerabilities, and virus attacks according to AFSSI 5021 (will convert to AFMAN 33-225, Volume 2).

2.11.3.16. Establishes restrictions on shared usage of programs or files.

2.11.3.17. Ensures site certification is obtained before operational use.

2.11.3.18. Ensures each information system operates within the constraints of the system security policy and network security policy.

2.11.3.19. Ensures measures exist to control access to information systems based on users' validated clearances, access approval for categories, and need to know.

2.11.3.20. Maintains information systems processing sensitive, classified, and critical information according to configuration management controls, and provides security guidance to the established configuration control board (CCB).

2.11.3.21. Identifies information ownership for each multi-user information system to include accountability, access rights, and special handling requirements.

2.11.4. Users:

2.11.4.1. Protect system information and resources according to established security policies and procedures.

2.11.4.2. Report system security incidents, vulnerabilities, and virus attacks according to AFSSI 5021.

Chapter 3

MINIMUM REQUIREMENTS

3.1. General. Safeguard computer systems and information against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons. Protect hardware, firmware, software, and information against unauthorized disclosure, destruction, or modification.

3.1.1. Prior to operating, certify and accredit all information systems according to **Chapter 4**.

3.1.2. Recertify and reaccredit all information systems every 3 years unless changes to the information system or environment baseline impact security, thereby necessitating recertification or reaccreditation sooner.

3.1.3. Implement a minimum of Class 2 (C2) functionality according to AFMAN 33-229, *Controlled Access Protection (CAP)*. (**NOTE:** C2, as used in this instruction, indicates the criteria class [controlled access protection] represented in DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985, and not command and control.)

3.1.4. DELETED.

3.2. Designated Approving Authority Assignment.

3.2.1. The host wing commander is the DAA for the base-wide area or metropolitan area network to include the core services (backbone [to include routers, switches, and hubs], boundary protection, E-mail, NT server farms), network infrastructure (to include workstations, printers and network devices, etc. regardless of ownership), and standalone systems for each installation; this authority will not be delegated.

3.2.1.1. DELETED.

3.2.1.2. The wing commander may appoint a DAA representative at each geographically separated unit (GSU) if the GSU's network boundary protection (i.e., firewall, intrusion detection) is provided by the host network control center. If the GSU is responsible for its own boundary protection the wing commander may delegate DAA authority to the ranking officer at the GSU. In this instance, further delegation is prohibited.

3.2.2. MAJCOM, FOA, DRU, and tenant unit commanders are DAAs for unique systems and networks they own and operate. This authority may be delegated to the 2-letter/deputy level MAJCOM functional office. This also applies to MAJCOM consolidated systems spread throughout their respective bases. MAJCOMs that expand their accreditation boundary to include all of their bases are the DAA for all of their bases. Further delegation is prohibited.

3.2.2.1. DELETED.

3.2.2.2. DELETED.

3.2.3. The Air Force Chief Information Officer (AF-CIO) is the responsible official for Air Force owned and operated functional systems in the Air Force enterprise. The Air Staff 2-letter director levels have DAA authority for their appropriate functional systems. This authority maybe delegated to their 3-letter director level. If the authority is delegated, they are the DAA for those functional systems

from cradle to grave. For example, for Integrated Logistics Systems-Supply, the HQ USAF/IL could delegate DAA authority to HQ USAF/ILS. Further delegation is prohibited.

3.2.4. The Administrative Assistant to the Secretary of the Air Force (SAF/AA) is the DAA for all information systems, regardless of classification, used inside Air Force Special Access Program/Special Access Required (SAP/SAR) programs and program facilities. This authority may be delegated to Air Staff offices responsible for the security of specific SAP/SAR programs. Further delegation may occur only with SAF/AA approval.

3.3. Controlled Access Protection Products.

3.3.1. Use computer-based security features to satisfy security requirements for information systems. Where computer-based security is not feasible, enhance existing safeguards and controls to satisfy security requirements according to AFMAN 33-229.

3.3.2. Evaluate, assess, or locally test and approve all hardware, software, and firmware products that provide security features prior to use on any accredited information system or network. Implement computer-based security solutions in the following order:

3.3.2.1. Use products evaluated by the National Computer Security Center (NCSC) listed on the Evaluated Products List.

3.3.2.2. Use products formally assessed by HQ AFCA listed on the Assessed Products List.

3.3.2.3. Select a suitable product, then test and certify its security features according to **Chapter 4**. Certification must validate claims that the security features meet Air Force and DoD security policy or that additional countermeasures are required.

3.4. Software Security.

3.4.1. Certify all software prior to installation and use on an operational accredited system. Follow the certification process outlined in **Chapter 4** and ensure DAA approval is granted. (***NOTE:*** Freeware, public domain software, and shareware originating from questionable or unknown sources, [e.g., non-DoD bulletin boards or World Wide Web sites, etc.] are much more susceptible to malicious logic and may violate the system security policy. Base use of such software on operational need.)

3.4.2. Avoid software development, testing, and debugging on operational information systems. If no alternate exists, meet the following conditions:

3.4.2.1. Protect applications and files from unauthorized disclosure.

3.4.2.2. Maintain the availability, confidentiality, integrity, and accountability of information system resources and information.

3.5. Personal Computers (PC) and Workstations. This section applies to all information systems used by only one individual at a time. The PC or workstation may be operated as a stand-alone system or connected in a network environment. (**NOTE:** Information systems that allow file sharing over a network must comply with the requirements of multi-user information systems [paragraph **3.6.**].)

3.5.1. Unclassified and Sensitive Processing:

3.5.1.1. Verify each user's need for access to information system resources and information. Follow identification and authentication procedures according to AFMAN 33-223, *Identification and Authentication*.

3.5.1.2. Confirm that information systems added to the network comply with the system security policy.

3.5.1.3. Protect against casual viewing of information by using password-protected screen savers when workstations are unattended.

3.5.1.4. Protect the information system and data against tampering. Provide protection from outsider threats by controlling physical access to the information system itself. Provide protection from insider and outsider threats by installing keyboard locks, basic input/output system (BIOS) passwords, password-protected screen savers, add-on security software, etc., or by establishing controls for removal and secure storage of information from unattended information systems. (**NOTE:** Using password-protected screen savers in conjunction with BIOS passwords affords maximum protection for sensitive information. Using screen saver alone provides minimal protection.)

3.5.1.5. Protect against unauthorized web browser access. Use protection measures in paragraph **3.5.1.4.** and use dynamic host Internet protocol addressing or local operating system security features to force each workstation to log onto the network before granting web access.

3.5.1.5.1. Disable ActiveX and Java features when visiting untrusted sites (non-.gov or -.mil sites). When mission accomplishment necessitates the need to enable these features, obtain DAA approval and update the SSAA.

3.5.1.6. Clear or destroy media used to store sensitive information before release to unauthorized personnel. Follow procedures in AFSSI 5020, *Remanence Security* (will convert to AFMAN 33-224).

3.5.1.7. DELETED.

3.5.2. Classified Processing. In addition to the security requirements in paragraph **3.5.1.**, the following security requirements apply:

3.5.2.1. Physically protect each network node to a level adequate for protecting the most restricted information accessible at the node.

3.5.2.2. Information systems using nonvolatile, nonremovable storage media must meet one of the following conditions:

3.5.2.2.1. Install the computer in an area approved for open storage of classified information at or above the highest classification level of the information processed.

3.5.2.2.2. Use an NCSC-evaluated, AFCA-assessed, or locally tested and DAA-approved product or technique to prevent storing classified information on nonvolatile, nonremovable storage media. Ensure product protects against inadvertently writing information to storage media.

3.5.2.3. Unless multi-level security (i.e., criteria class B) is implemented according to DoD 5200.28-STD, ensure all personnel authorized to use the information system are cleared to the highest level and most restricted category of information contained in the information system.

3.5.2.4. Use a separate copy of the operating system and other necessary software for each level of classification on information systems employing periods processing.

3.5.2.5. Clear equipment and media when changing modes of operation or changing operations to the same or higher classification level. Sanitize storage devices that contain classified information before using at a lower classification level according to AFSSI 5020.

3.5.2.6. Safeguard, mark, and label output products and removable media according to DoDD 5200.1, *DoD Information Security Program*, December 13, 1996; and AFI 31-401, *Information Security Program Management*.

3.5.2.7. Provide internal markings on files to indicate the information sensitivity level and any special handling instructions, where practical.

3.5.3. Guidance on the use of personal digital assistants (PDA):

3.5.3.1. A PDA is an automated information system and therefore is subject to Air Force policy and guidance governing the security and use of a desktop or notebook computer.

3.5.3.2. Use of PDAs (e.g., Palm Pilot® or Cassiopeia® devices) within the Air Force has increased significantly. This family of devices offers personal productivity enhancements, particularly by making certain features of the desktop environment portable (e.g., Microsoft Outlook® contacts, notes, appointments, and E-mail); however, the use of some products and features introduces security risks to information systems and networks.

3.5.3.3. Individuals may use PDAs to:

3.5.3.3.1. Process unclassified information from desktop workstations. This includes the following typical features: schedules, contact information, notes, E-mail, and other items.

3.5.3.3.2. Take notes, save information, or write E-mails, when away from desktop workstations, whether down the hall or out of the country.

3.5.3.3.3. Synchronize information with desktop workstations.

3.5.3.4. Do not use PDAs for the following:

3.5.3.4.1. Do not process or maintain classified information. There are currently no approved methods for clearing (sanitizing) classified information from these devices. If contaminated, security personnel must protect, confiscate, or possibly destroy the affected PDA.

3.5.3.4.2. Do not connect or subscribe to commercial internet service providers (ISP) for official E-mail services (e.g., Palmnet® wireless communications service). The use of commercial ISPs for official business is not allowed due to the high operational risk posed by the possible collection of sensitive information.

3.5.3.4.3. Do not synchronize information across a network using a wireless connection. The configuration required to permit this functionality introduces unacceptable risks into a network--opening firewall ports and sending passwords in the clear. Exceptions to this restriction will be evaluated on a case-by-case basis and require local DAA approval.

3.5.3.5. Software security restrictions described in paragraph **3.4.** apply to these devices.

3.5.3.6. The only authorized connection through a PDA modem is to an official Air Force remote access server (RAS) account protected by an authorized network control center firewall. Do not synchronize the PDA remotely by direct dial-in access to desktops.

3.5.3.7. Do not issue users a PDA until they agree, at a minimum, to the terms outlined in paragraph **3.5.3.**

3.5.3.8. You can find additional security related information on PDAs at the AFCA product evaluation webpage (**http://www.afca.scott.af.mil/prodeval**).

3.5.3.9. The following applies to handling and controlling of PDAs:

3.5.3.9.1. Disable auto sync on the desktop application menu until needed. Once the PDA and computer have synced up, turn off the auto-sync.

3.5.3.9.2. Password protect PDAs according to AFMAN 33-223, if technically possible. If the PDA is technically unable to use a password, increase physical access controls to prevent unauthorized access.

3.5.3.9.3. Disable infrared (IR) port beaming capability. If the IR port is unable to be disabled, cover the IR port with a visor or similar object (i.e., tape).

3.5.3.9.4. Turn off PDAs when not in use.

3.5.3.10. Include PDAs in the SSAA for the network. Ensure vulnerabilities associated with the PDAs are included in the threat and vulnerability assessment. Reflect the handling, controlling and usage of PDAs in the network security policy.

3.5.3.11. Connecting privately owned PDAs to the Air Force network is strongly discouraged. If individuals have a requirement to use a PDA on the Air Force network, they must request issuance of a government-owned PDA. Privately owned PDAs will not be connected to the Air Force network without sufficient justification and the DAA approval. Justification must include mission requirements, government availability, and rationale of how duty position will be enhanced. Include handling of privately owned PDAs and software in the SSAA. Individuals must sign a PDA usage statement (**Attachment 3**) agreeing to the terms outlined in this instruction.

3.5.3.12. Do not use PDAs in classified environments because of their infrared and similar recording capabilities. PDAs (includes privately owned) contaminated with classified information will be confiscated and possibly destroyed, since there is currently no means to sanitize the PDA.

3.6. Multi-User Information Systems. This section applies to all multi-user file servers (e.g., file transfer protocol [FTP]), network file servers, World Wide Web servers, etc.), and information systems that permit file sharing, perform network security functions, or provide security services (e.g., Automated Security Incident Monitoring [ASIM], firewalls, etc.). AFI 33-115V1 directs that all communications and information services entering and exiting the base or site fall under the operational control of the NCC. Follow AFIWC and AFCA guidance on implementing network boundary protection to include the ASIM system, installing and configuring firewalls, and disabling system services (e.g., Barrier Reef “How to Guides”). AFSSI 5027 provides additional guidelines for securing computer networks.

3.6.1. Unclassified and Sensitive Processing. In addition to the security requirements listed in paragraph **3.5.1.**, the following security requirements apply. If conflicts develop, the following requirements take precedence:

3.6.1.1. Adhere to AFMAN 33-223 to ensure individual accountability and use of proper identification and authentication (I&A) procedures, and verify access.

3.6.1.2. Control access to files, software, and devices so that only authorized users can use them.

3.6.1.3. Control access to prevent unauthorized persons from using network facilities.

3.6.1.4. Use network components (e.g., trusted routers, bastion hosts, gateways, firewalls, etc.) or information systems that enforce mandatory access control and I&A to provide access controls.

3.6.1.5. Provide each user with only those system privileges needed for assigned tasks (least privilege concept).

3.6.1.6. Limit access to privileged programs (i.e., operating system, system parameter and configuration files, and databases), utilities (i.e., assemblers, debuggers, maintenance utilities), and security-relevant programs/data files (i.e., security monitor, password files, and audit files) to authorized personnel (i.e., system administrator and ISSO).

3.6.1.7. Limit the capability to conduct privileged actions (i.e., loading new users, password management, modifying and patching system routines or files, examining memory locations, real-time monitoring of user activities, and initiating or executing privileged routines) to authorized personnel.

3.6.1.8. Implement auditing according to AFMAN 33-229 for C2 criteria class information systems. Information systems operating at higher criteria classes will implement audit requirements according to DoDD 5200.28-STD.

3.6.1.8.1. Establish an audit record capable of tracing network activity and actions to an individual user.

3.6.1.8.2. Ensure the audit mechanism records any event that attempts to change the security profile (e.g., access controls, security level of the subject, user password, etc.).

3.6.1.8.3. When technically feasible, ensure the information system aborts or suspends unauthorized user activity when detected, unless performing real-time analysis.

3.6.1.9. Generate output only within the central facility or at a remote station staffed with personnel cleared for the highest sensitivity level of information processed by the information system when the system does not have controls that limit output to authorized users.

3.6.1.10. Implement normal building and area entry controls (i.e., physical, administrative, and personnel security) at remote terminal sites when host systems have adequate internal access controls. Disable communications lines and take other necessary actions to protect information, systems, and resources when adequate internal controls do not exist.

3.6.1.11. Protect transmission of classified, sensitive, or a combination of classified and sensitive information according to AFI 33-201, *(FOUO) Communications Security (COMSEC)*.

3.6.2. Classified Processing. In addition to the security requirements listed in paragraph **3.5.** and paragraph **3.6.1.**, the following security requirements apply. If conflicts develop, the following requirements take precedence:

3.6.2.1. Where the facility (building and room) plays a major role in providing security for information systems, establish procedures to notify IA personnel of impending changes to the facility.

3.6.2.2. Operate networks in a system high or dedicated security mode unless all network nodes are accredited for operation in the multilevel or partitioned security mode.

3.6.2.3. Adhere to the DISA Connection Approval Process if the system is connected to SIPRNET.

3.6.2.4. Use only Secret and Below Interoperability (SABI)-approved devices and adhere to SABI configuration guidelines when connecting classified systems or networks to unclassified systems or networks.

3.7. Requirements for Foreign National Access to Unclassified But Sensitive Internet Protocol Router Network (NIPRNet).

3.7.1. Requests to grant foreign national access to information systems and networks by foreign governments, allied and coalition organizations are handled as follows: the wing commander sends the request to the MAJCOM/CC who verifies the need, then forwards it to HQ USAF/SC for Air Force approval; it is then validated by the Joint Staff/J6 and approved/disapproved by the Office of the Secretary of Defense (OSD).

3.7.1.1. DELETED.

3.7.1.2. DELETED.

3.7.1.3. DELETED.

3.7.1.4. DELETED.

3.7.2. Provide the following information in the request to OSD for foreign national access approval:

3.7.2.1. Mission Statement and description of current environment.

3.7.2.2. Organizations involved and POCs.

3.7.2.3. Type of connectivity required (e.g., HTTP, Simple Mail Transfer Protocol, FTP, etc.)

3.7.2.4. What type of information and how often information will be transmitted.

3.7.2.5. Verification that foreign disclosure has been made by the appropriate DAA.

3.7.3. Request to grant foreign national access to information systems and networks to the following category of individuals is based on the access needed and is approved by the Approving Authority stated in **Table 3.1.** The Approving Authority approves access for the following individuals:

3.7.3.1. Assigned to the Defense Personnel Exchange Program.

3.7.3.2. Assigned to the Cooperative Program.

3.7.3.3. Employed Overseas by the U.S. Government under Status of Forces Agreement.

3.7.3.4. Assigned to CONUS based North American Aerospace Defense Command (NORAD).

3.7.3.5. Employed CONUS by the U.S. Government.

3.7.3.6. Foreign Military personnel temporarily assigned to Air Force-sponsored training programs (i.e., Air Force Academy, Air Education and Training Command (AETC) training courses, medical students, etc.)

3.7.3.7. Employed overseas by foreign national contractor.

3.7.3.8. Individuals assigned to the Foreign Liaison Officer Program.

Table 3.1. Approving Authority for Foreign National Access.

Access Needed	Approving Authority
E-mail (1)	Local Host Wing DAA
Stand alone and networks within a local enclave	
NIPRNet (2)	MAJCOM CC/CV
Functional System Access	DAA of System

NOTES:

1. E-mail accounts of foreign nationals must identify the individuals as foreign personnel to include position assigned. Example: lastname, firstname, rank, country of origin-assignment, office symbol; Doe, John, WG CDR, UK-FLO, CENTAF/A6.
2. Does not constitute full NIPRNet access, controls must be in place to ensure only authorized sites are accessed.

3.7.4. Once approved, grant network access (to include (NIPRNet)) to these individuals and limit access to the extent necessary to perform assigned duties. ***NOTE:*** Approval to access the NIPRNet or other networks by foreign personnel does not equate to authority to exchange data or access systems located on that network. The system DAA grants access to the information systems and Designated release/disclosure authority grants access to information.

3.7.4.1. DELETED.

3.7.5. Before authorizing foreign national access to information supervisors will:

3.7.5.1. Identify specific information system access requirements for the position.

3.7.5.2. Work with the unit COMPUSEC manager (UCM) and ISSO to implement necessary controls to assure that only authorized information systems are accessible by approved personnel, as defined by the foreign disclosure officer.

3.7.5.3. Ensure that access to any unclassified information system or web site containing information that is controlled under the Arms Export Control Act, Privacy Act, and exemptions to the Freedom of Information Act are approved by the system DAA/webmaster and the local foreign disclosure officer.

3.7.5.4. Ensures security measures employed adhere to information assurance policy.

3.7.6. In addition, foreign nationals who have access to specific information contain within a functional system, the local DAA will ensure:

3.7.6.1. The information is properly processed for disclosure.

3.7.6.2. The local foreign disclosure officer validates that these requirements fall within the limits of the disclosure authority approved for the position.

3.7.6.3. The SSAA for the system is updated to reflect foreign national access.

3.7.7. Foreign Nationals who are permanent residents of the U.S have the same status as U.S. citizens and are exempt from these procedures.

3.8. Configuration Management.

3.8.1. Use configuration management to ensure the integrity of critical functions in security-related hardware, firmware, and software of all information systems. Distributing hardware, firmware, and software under configuration management control shall be provided an appropriate level of protection to assure product integrity. Use the computer resources life-cycle management plan and the CCB to ensure system integrity throughout the life cycle of an information system.

3.8.2. Ensure interoperability and compatibility with existing Air Force standard network security policies and procedures according to the Joint Technical Architecture-Air Force.

3.9. Remote Access via Modem.

3.9.1. Centralize modem management under the NCC according to AFSSI 5027. Do not use modems in any PC or laptop computer while physically connected to the base network. Stand-alone PCs may use modems when approved by the DAA (i.e., Bulletin Board).

3.9.2. The security requirements (e.g., I&A, audit, etc.) of the local information system also apply to systems allowed to remotely access that information system.

3.9.3. Make sure that access tables, when used, remain current.

3.9.4. Prohibit the use of call-forwarding capabilities when using callback or dialback technology.

3.9.5. Annotate remote access in the audit logs.

3.9.6. Do not publicize telephone numbers to anyone other than those with a need to know.

3.9.7. Employ methods for controlling access (e.g., callback, token generation, etc.) where the capability exists.

3.10. Using Hardware or Software Not Owned by the Air Force.

3.10.1. Contractor-Owned. Contractor-owned or -operated hardware and software must meet all security requirements for government-owned hardware and software. AFI 31-601, *Industrial Security Program Management*, provides security policy and guidance relating to contractor actions involving classified information. DoD Manual 5220.22 (DoD 5220.22-M), *National Industrial Security Program Operating Manual*, January 1995, applies to off-base contractor information systems and on-base contractor facilities when the Air Force does not have responsibility for industrial security inspections. If DoD 5220.22-M applies, Defense Investigative Service approval is mandatory before processing classified information. If the contractor must comply with this instruction instead of the manual, the Air Force must provide the contractor with specifications that establish contractor and Air Force responsibilities for security, including who should conduct the information system C&A and who the DAA is for the system. The program or project manager, contracting or procurement officer, and appropriate COMPUSEC personnel should jointly develop this guidance.

3.10.2. Other Service or Agency Owned (**NOTE:** Where a lead service is other than the Air Force, some protection requirements may not be achievable). Develop an agreement before using equipment and facilities owned or operated by other services or agencies to ensure:

3.10.2.1. Air Force use of other services' or agencies' resources does not degrade the required security posture.

3.10.2.2. Mission-critical processing takes priority.

3.10.2.3. The lead service (in joint-service activities) identifies the DAA for the information system and determines security requirements for the information systems supporting the activity.

3.10.2.4. Satisfying Air Force requirements in this instruction for the protection of Air Force information.

3.10.3. Foreign Owned. Do not use foreign-owned or -operated (e.g., joint/coalition) information systems to process sensitive or classified information or for critical processing, unless required by international treaties or security agreements.

3.10.4. Personally Owned. Do not use personally owned information systems (i.e., hardware or software) to process classified information. Using personally owned hardware and software for government work is strongly discouraged; however, it may be used for processing unclassified and sensitive information with DAA approval (see AFI 33-112, *Computer Systems Management*; and AFI 33-114, *Software Management*). (***NOTE:*** Document blanket approvals for the purpose of telecommuting in a local operating instruction.) Approved personally owned information systems contaminated with classified information will be confiscated. Base approval on the following requirements:

3.10.4.1. The written approval specifies the conditions under which the information system operates.

3.10.4.2. When using a personally owned information system for official work, the system must employ anti-virus software, government-owned sensitive information must remain on removable media, and government-owned sensitive information must be marked and protected according to the sensitive category (e.g., Privacy Act, For Official Use Only [FOUO], etc.) program directives.

3.11. Controlling Maintenance Activities.

3.11.1. Restrict information system maintenance to authorized personnel with a security clearance for the highest classification and most restricted category of information processed. Uncleared individuals may perform maintenance on information systems used to process classified information only if the information is purged or an appropriately cleared individual (capable of identifying unauthorized activity) observes their actions.

3.11.2. Allow remote software diagnostics or maintenance only if the information system audits such activities or an appropriately cleared individual (capable of identifying unauthorized activity) observes such activities. When maintenance activities are suspended or completed, disconnect or disable access to the information system. Additionally, verify the identity of the maintenance personnel to prevent the unauthorized disclosure of sensitive and classified information.

3.11.3. Prevent vendor maintenance personnel from removing classified or sensitive media, products, etc., from government facilities when those personnel do not have the proper authorization (e.g., verified identity, security clearance, access approval for categories, need to know) to access that media. Before releasing an information system component containing nonvolatile storage media (e.g., tapes, disks, battery-powered random access memory, etc.) to uncleared maintenance activities, sanitize the component of classified and/or sensitive information according to AFSSI 5020.

3.12. Requirements for Foreign National Access to SIPRNet. Request Joint Staff/J6 validation and OSD approval in order to connect to DISN-SIPRNET (use the same process listed in paragraph **3.7.1.** to obtain approval). The request must include items identified in the draft DISA Connection Approval Process (i.e., mission statement, organizations involved, POC, brief description of current environment to include topology, consent-to-monitor statement, etc.). The technical solution must include a high assurance guard in United States-controlled space to protect United States-only information and information systems. The Certifier must submit the SSAA to DISA and present the technical solution to the DISN Security Accreditation Working Group (DSAWG). If approved, the DSAWG advises the sponsoring Commander-in-Chief (CINC), Air Force and DISA, in writing, so DISA can grant the approval to connect.

3.13. Malicious Logic Protection. Protect information systems (including network servers) from malicious logic (e.g., virus, worm, Trojan horse, etc.) attacks. Apply an appropriate mix of preventive measures to include user awareness training, local policies, configuration management, and anti-virus software. At a minimum:

3.13.1. Implement anti-virus software on all information systems and networks.

3.13.1.1. Use only anti-virus tools and signature files/datfiles obtained from the AFCERT FTP or DoD Computer Emergency Response Team (CERT) web sites. NCCs will direct configuring (where technically feasible) the signature file update routine to an NCC-controlled site inside the base security perimeter.

3.13.1.1.1. If a waiver is required to use other than DoD anti-virus software, forward requests through your chain of command to HQ AFCA/GCI for approval or disapproval.

3.13.1.2. Activate anti-virus software during AIS use (auto-defend or auto-protect must be enabled to allow a scan when a file is run, opened, copied, moved, created, or downloaded).

3.13.1.3. IA or IPO personnel will check for anti-virus signature files/datfiles updates daily from the AFCERT/DoD CERT sites. Users will schedule ‘Live Updates’ daily to pull down new signature files from the NCC-controlled site or NCC’s site will replicate (if feasible) new signature files to the users as soon as received. A virus scan will be accomplished immediately following an update of a signature file.

3.13.1.4. Establish procedures to rapidly obtain, distribute, and install changes to anti-virus software on all information systems (including network servers).

3.13.2. Where feasible, scan all incoming traffic and files for viruses at the network server level.

3.13.3. Scan removable and fixed media:

3.13.3.1. Scan fixed media daily on the core network services listed in AFI 33-115V1, to include all multiuser file servers (e.g., FTP, WWW, network file servers, etc.).

3.13.3.2. The wing DAA (host wing commander) is responsible for establishing the local virus scanning frequency for fixed media on noncore service computing devices (e.g., laptops, desktop computers). The time period between scans will not exceed 7 calendar days. If a local scanning frequency is not established in the host wing's system security policy, scan all fixed media daily.

3.13.3.3. Scan removable media for viruses before each use, which can be automated if anti-virus software is configured properly.

3.13.4. Report all virus attacks according to AFSSI 5021.

3.13.5. DELETED.

3.13.6. DELETED.

3.13.7. Preserve malicious logic reports as evidence for ongoing investigations.

3.13.8. Include virus prevention, detection, eradication, and reporting procedures in user training.

3.14. Training. License network users according to AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*. The wing IA office trains UCMs on this instruction, identification and authentication, remanence security, vulnerabilities and incidents reporting, etc.

3.15. Notice and Consent for Information System Monitoring. Information systems are subject to monitoring by authorized personnel. Display warning banners according to AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*.

3.16. Reporting:

3.16.1. Report information system accreditation according to AFI 33-205.

3.16.2. Report information system vulnerabilities, security incidents, and virus attacks according to AFSSI 5021.

3.17. Wireless Local Area Networks (WLAN).

3.17.1. Apply the following security requirements to wireless solutions. WLANs are susceptible to interference and are easily jammed:

3.17.2. All existing WLANs operating prior to 1 June 2001 may continue to operate; however, the responsible DAA must provide a migration plan to ensure the systems meet the requirements by 1 January 2003. Air Force unclassified networks will be enabled for hardware token, certificate-based access controls no later than October 2002.

3.17.2.1. WLAN solutions must meet the same C&A requirements as wired LAN solutions, according to **Chapter 4**. Program Management Offices must consider these requirements during the development of a WLAN solution.

3.17.2.2. Engineer WLAN solutions to preclude backdoors into the Air Force enterprise network.

3.17.2.3. Configure wireless equipment for appropriate local area network (LAN) security options. Commercial-off-the-shelf products typically arrive with factory default settings, which may not offer LAN security.

3.17.2.4. Use encryption standards to protect information accordingly. Encrypt all radio frequency wireless networks according to AFI 33-201. Comply with AFSSI 7010, *(S) Emission Security Assessment (U)* (will convert to AFMAN 33-214V1), for WLANs.

3.17.2.5. Use National Institute of Standards and Technology (NIST) standard, Federal Information Processing Standards (FIPS) Pub 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001, Triple data encryption standard encryption, or the new NIST advanced encryption standard (expect FIPS publication April-June 2001) for encryption of sensitive information.

3.17.2.6. Ensure that a user cannot enter a WLAN without strong authentication. As a minimum, strong authentication should include an extended service set identifier and mandatory access control (MAC) address identification with an integrity lock.

3.17.2.7. Use Institute of Electrical & Electronics Engineers (IEEE) 802.11 standard for WLANs using the Direct Sequence Spread Spectrum (less susceptible to jamming, better throughput) or Frequency Hopping Spread Spectrum (more difficult to intercept) standards.

3.17.2.8. Coordinate use of any wireless device, including commercial nonlicensed devices, with the local Air Force frequency manager. Coordinate any use in foreign nations with the United States Military Communications-Electronic Board (USMCEB) on a system specific basis, for spectrum supportability determination. Supportability alone will not authorize approval to operate the system. A frequency assignment is required from the host nation prior to equipment usage. The local frequency manager can assist with processing a spectrum supportability determination from the USMCEB and processing a frequency assignment request from the host nation. Use of wireless devices may not be approved for use in another country, since each country allocates its frequency resources differently. This can also be an issue in the CONUS. Also, if a nonlicensed WLAN interferes with licensed equipment, i.e., medical equipment, Federal Communications Commission regulations require the WLAN to shut down. ***NOTE*:** If a private WLAN interferes with a federal WLAN, the federal WLAN must accept the interference. If a federal WLAN interferes with a private WLAN the federal WLAN must shut down. See AFI 33-118, *Radio Frequency Spectrum Management,* for more information.

3.17.2.9. Certify all wireless devices for spectrum supportability prior to obligating funds according to AFI 33-118.

3.17.2.10. Use replaceable WLAN radios (Personal Computer Memory Card International Associate [PCMCIA] or PC cards) in all devices attached to WLAN.

3.17.2.11. Comply with AFMAN 33-120, *Radio Frequency (RF) Spectrum Management*, which prohibits the use of WLANs for critical or command and control systems.

3.17.2.12. Ensure continuity of operations plans include using alternative manual procedures in case of automated system failure.

3.17.2.13. Conduct a risk analysis to determine the information intercept and monitoring vulnerabilities (e.g., electronic emanations, emission security [EMSEC], etc.), prior to implementing WLANs. Review all EMSEC assessments on all classified systems within the same building or within 20 meters of any components of the WLAN before beginning engineering, installation, or ordering the LAN.

3.17.2.14. Ensure that the administrators have the capability to audit or monitor the WLAN to detect intrusions. Intrusions are not always detected immediately. If logs are not available, it will be difficult to troubleshoot unauthorized access.

3.17.2.15. Remotely configure access points on the wired side of the WLAN configuration. This will prevent an intrusion on the wireless side from intercepting configuration information and changing the WLAN settings.

3.17.2.16. Simple Network Management Protocol is often used to remotely configure an access point. Change default community strings to prevent unauthorized configuration (read and write privileges to access point).

3.17.2.17. Ensure unused protocols are filtered at the access point. This will enhance the security and efficiency of the WLAN.

3.17.3. Consider the following characteristics and parameters of wireless solutions prior to the use of any wireless solution:

3.17.3.1. Wireless solutions may create backdoors into Air Force LANs. If a device receives information via a wireless technology and that device allows that information to be placed directly into the LAN via cable at the workstation level, then all perimeter and host-based security devices may have been bypassed.

3.17.3.2. When utilizing a wireless LAN solution the LAN card's unique numeric identifier (MAC address) can be copied electronically (spoofed). It is important to ensure strong authentication, i.e., PKI or FIPS compliant device or SECNET 11. The user cannot rely totally on MAC address resolution as the only means for authentication.

3.17.3.3. Wireless LANs are susceptible to interference, interception, and are easily jammed. Clearly define standards and publish WLAN security policies in the network security policy.

Chapter 4

CERTIFICATION AND ACCREDITATION

4.1. Background . The Computer Security Act of 1987 established the requirement for every information system to be certified and accredited.

4.1.1. For several years, AFSSI 5024 was the guidance by which Air Force information systems were certified and accredited. In order to fall in line with the other DoD services, the Air Force is transitioning to the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). DoDI 5200.40, *Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)* (will become DoDI 8510.1), implements guidance to standardize the Certification and Accreditation (C&A) process throughout the DoD. DoD 8510.1-M, *Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual,* is the application manual that explains the step-by-step process on how to accomplish C&A using the DITSCAP. See **Table 4.1.** for a cross-reference from old terms to the new terms.

4.1.2. Effective 1 April 2001, use DITSCAP to certify and accredit new systems or existing systems that have not been previously certified and accredited. For those systems that are actively working the C&A process (prior to 1 April 2001 and in AFSSI 5024 Phase II or higher), may complete the C&A process using AFSSI 5024. Systems in spiral development will transition to DITSCAP no later than 1 April 2002. Systems that have completed a C&A process according to AFSSI 5024, will transition to DITSCAP when recertification or reaccreditation is required.

Table 4.1. Cross-Reference of Old Terms with the New Terms

Old Term	New Term
System Program Office (SPO)	Program Manager
Single Manager (SM)	
Certifying Official	Certifier
Computer Systems Security Officer (CSSO)	Information Systems Security Officer (ISSO)
Full Accreditation	Accreditation
Interim Accreditation	Interim Approval to Operate (IATO)
C&A Package	System Security Authorization Agreement (SSAA)

4.2. Roles and Responsibilities . Key roles and responsibilities in the DITSCAP process include the DAA, Certifier, Program Manager, User Representative, and the ISSO. Some of these key roles are explained in **Chapter 2** of this instruction and additional information is contained in Chapter 8 of DoD 8510.1-M. There are numerous other personnel and agencies that support the C&A tasks. The number of participating organizations and their assignments will differ between programs based on the guidance set forth by the DAA, availability of resources, level of effort for certification, the security requirements, as well as the sensitivity and criticality of the system. It is equally important to identify their roles and responsibilities early on and include this information in the SSAA. In addition, the following information is provided as an overview of *typical* assignments of responsibilities to the various participants.

4.2.1. Designated Approving Authority (DAA). This person has the largest effect on the scope of C&A work. See paragraph **2.7.** for the DAA roles and responsibilities.

4.2.1.1. DAA Representative. To ease the burden of dealing with the day-to-day issues of accrediting information systems, the DAA may appoint a representative to perform many of the duties. The DAA Representative remains actively involved in certification tasks and keeps the DAA informed of major issues. They identify, address, and coordinate security accreditation issues with the DAA. A direct link must exist between the DAA Representative and the DAA. However, the DAA, not the DAA Representative, makes the accreditation decision.

4.2.1.2. DAA Liability. It is imperative that the DAA understands the legal ramifications of signing the accreditation document. They ensure that the appropriate security measures, documentation, and the C&A process are implemented and maintained throughout the life cycle of the information systems.

4.2.1.2.1. When granting approval to operate, the DAA accepts the ultimate responsibility for its operation and officially declares:

4.2.1.2.1.1. The specified system adequately protects the information or resources.

4.2.1.2.1.2. Acceptance of the residual risks involved in operating the system.

4.2.1.2.2. Maintain sufficient documentation to support the DAA's accreditation decision as well as to verify the implementation and operational maintenance of designated security measures or system safeguards.

4.2.1.3. DAA Training. DAAs need to familiarize themselves with responsibilities, directives, regulations, and laws applicable to C&A, before initiating the C&A process.

4.2.2. Certifier. The Certifier is crucial to the success of the entire C&A effort. See paragraph **2.8.** for the Certifier's roles and responsibilities.

4.2.3. Program Manager. The program manager coordinates all aspects of the system from initial concept, through development, to implementation, and system maintenance. The program manager performs roles of the Single Manager listed in paragraph **2.5.3.**

4.2.4. User Representative. The user representative is the liaison for the user community throughout the life cycle of the system. The user representative defines the system's operations and functional requirements and is responsible for ensuring that the user's operational interests are maintained throughout system development, modification, integration, acquisition, and deployment. See DoD 8510.1-M, Chapter 8 for additional roles and responsibilities.

4.2.5. Information System Security Officer (ISSO**).** The ISSO assists in the development of the system security policy and ensures compliance on a day-to-day basis. Their most important role is during the Post-Accreditation Phase where they ensure the security posture of the system and the accreditation is maintained. They also perform roles identified in paragraph **2.11.3.**

4.2.6. Other Roles.

4.2.6.1. Certification Team. Working for the Certifier, the Certification Team accomplishes C&A according to the DITSCAP. Team members evaluate the technical and nontechnical features of the system to determine the level of protection provided and document their findings. Each member is responsible to the Certifier for the evaluations they perform and the documentation they submit.

The composition and size of the team will depend on the size and complexity of the system. Compose the team of members that have composite expertise in the whole span of activities requirement and who are independent of the system developers or project manager.

4.2.6.2. System Security Working Group (SSWG). This group directs security tasks, and identifies and resolves security-related issues throughout the system life cycle according to AFI 31-702. The group provides continuity among the system security policy, the system design, and the security engineering approach.

4.3. System Security Authorization Agreement (SSAA). The SSAA is the depository of evidence showing that the system meets the system security policy, all certification tasks are properly completed, the system is approved to operate, and a plan for maintaining the accreditation exists.

4.3.1. SSAA Outline. Use the SSAA outline in DoD 8510.1-M, Appendix 1. List all items in the SSAA outline. For those items that do not apply, list the outline number, the detailed description, and then N/A. Refer to Table A2.1 for a chart that references the task with the specific paragraph in DoD 8510.1-M.

4.3.1.1. In addition to Appendices A through R required by DoD 8510.1-M, the Air Force requires the additional mandatory appendices:

4.3.1.1.1. Appendix S - Certificate of Networthiness/Networthiness Recommendation.

4.3.1.1.2. Appendix T - Minimal Security Activity Checklists.

4.3.1.1.3. Appendix U - Network Vulnerability Assessment Reports.

4.3.1.1.4. Appendix V - Trusted Facility Manual (TFM).

4.3.1.1.5. Appendix W - Security Features User's Guide (SFUG).

4.3.1.2. MAJCOMs may require additional appendices to meet specific needs. Include all documentation that is relevant to the C&A process.

4.3.2. Automated Tools. DISA provides an automated tool to aid in the preparation of the SSAA, which can be downloaded from **https://www.afca.scott.af.mil/ip/compusec/cna/cna.htm**.

4.3.3. Accreditation Boundaries.

4.3.3.1. Networks. When accrediting a network, it is not necessary to certify individual workstations on the system. Include the workstations in the network description, as long as all of the workstations contain similar software and hardware.

4.3.3.2. Systems. A system can be as small as a stand-alone workstation or as large as a complete network, with servers, router, hubs, workstations, etc. Software requires a platform (hardware) in order to operate. Certify the environment in which the software is operating. The software and hardware are accredited together as a system.

4.3.4. Security Test and Evaluation (ST&E). Use only JTA-AF approved software during ST&E.

4.4. Accreditation/Interim Approval to Operate (IATO). The decision to grant an accreditation, IATO, or disapproval is based on both the Certifier's recommendation and Certificate of Networthiness recommendation.

4.4.1. Accreditation. Accreditation is the formal declaration by the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards and controls; not to exceed 3 years. ***NOTE:*** Only an IATO can be issued if a Certificate of Networthiness is issued with conditions.

4.4.2. Interim Approval to Operate (IATO). The system does not meet the requirements as stated in the SSAA. Mission criticality mandates the system become operational and no other capability exists to adequately perform the mission. The IATO is a temporary approval issued for the minimal period of time necessary to meet all SSAA requirements (to achieve accreditation); not to exceed 1 year.

4.5. Site Certification.

4.5.1. Conduct site certification for systems that have a Certificate of Networthiness, a Certificate to Operate, or have a type accreditation signed by the functional DAA. The system still requires a site certification upon its arrival at the site.

4.5.2. Site certification provides assurance that the operational location has implemented the required security measures. This evaluation ensures that the integration and operation of the system in accordance with its certified design and operational concept pose an acceptable risk to the information being processed.

4.5.3. Site certification consists of:

4.5.3.1. Conducting the Site Accreditation Survey Checklist (See DoD 8510.1-M, Table AP2.T12).

4.5.3.2. Reviewing the local threats and vulnerabilities.

4.5.3.3. Testing the system installation and security configuration.

4.5.4. After considering the site certification evidence the local Certifier documents the evidence in the SSAA. The local DAA (wing commander) then signs, verifying that the system is installed and operated according to the SSAA.

JOHN L. WOODWARD, JR., Lt Gen, USAF
DCS/Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

CJCSI 6211.02A, *Defense Information System Network and Connected Systems*, 22 May 1996

CJCSI 6740.01, *Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations*, 18 September 1996

Information Technology Management Reform Act (ITMRA) of 1996

DoDD 5200.1, *DoD Information Security Program*, December 13, 1996

DoDI 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*, December 30, 1997

DoDD 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988

DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985 (commonly referred to as the Orange Book)

DoD 5220.22-M, *National Industrial Security Program Operating Manual*, January 1995

DoD 7740.1-G, *Department of Defense ADP Internal Control Guideline*, July 1998

DoD 8510.1-M, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, July 31, 2000

OMB Circular A-130, *Management of Federal Information Resources*

OMB Bulletin 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 23 March 1994 as amended through 7 December 1998

P.L. 100-235, *Computer Security Act of 1987*

Title 5 U.S.C. Section 552a (Privacy Act)

FIPS Pubs 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001

AFI 25-201, *Support Agreements Procedures*

AFI 31-401, *Information Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFI 31-702, *System Security Engineering*

AFPD 33-2, *Information Protection*

AFI 33-112, *Computer Systems Management*

AFI 33-114, *Software Management*

AFI 33-115V1, *Network Management*

AFI 33-115V2, *Licensing Network Users and Certifying Network Professionals*

AFI 33-118, *Radio Frequency Spectrum Management*

AFI 33-201, *(FOUO) Communications Security (COMSEC)*

AFI 33-205, *Information Protection Metrics and Measurements Program*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFMAN 33-120, *Radio Frequency (RF) Spectrum Management*

AFMAN 33-223, *Identification and Authentication*

AFMAN 33-229, *Controlled Access Protection (CAP)*

AFI 65-201, *Management Control*

AFDIR 33-303, *Compendium of Communications and Information Technology*

AFSSI 5020, *Remanence Security* (will convert to AFMAN 33-224)

AFSSI 5021, *Vulnerability and Incident Reporting* (will convert to AFMAN 33-225V2)

AFSSI 5024V1, *The Certification and Accreditation (C&A) Process*

AFSSI 5024V2, *The Certifying Official's Handbook*

AFSSI 5024V3, *The Designated Approving Authority's Handbook*

AFSSI 5024V4, *Type Accreditation*

AFSSI 5027, *Network Security Policy*

AFSSI 7010, *(S) Emission Security Assessment (U)* (will convert to AFMAN 33-214V1)

Abbreviations and Acronyms

ACC—Air Combat Command

ADP—Automated Data Processing

AETC—Air Education and Training Command

AFCA—Air Force Communications Agency

AFCERT—Air Force Computer Emergency Response Team

AF-CIO—Air Force Chief Information Officer

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AFMAN—Air Force Manual

AIA—Air Intelligence Agency

AFMC—Air Force Materiel Command

AFPD—Air Force Policy Directive

AFSSI—Air Force Systems Security Instruction

ASIM—Automated Security Incident Monitoring

BIOS—Basic Input/Output System

C2—Class 2 (Controlled Access Protection)(a division and class of DoD 5200.28-STD

C&A—Certification and Accreditation

CCB—Configuration Control Board

CERT—Computer Emergency Response Team

CINC—Commander-in-Chief

CIO—Chief Information Officer

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

COMPUSEC—Computer Security

COMSEC—Communications Security

CONUS—Continental United States

CSO—Communications and Information Systems Officer

DAA—Designated Approving Authority

DAC—Discretionary Access Control

DISA—Defense Information Systems Agency

DISN—Defense Information Systems Network

DITSCAP—DoD Information Technology Security Certification and Accreditation Process

DoD—Department of Defense

DoDD—Department of Defense Directive

DRU—Direct Reporting Unit

DSAWG—DISN Security Accreditation Working Group

EMSEC—Emission Security

FIPS—Federal Information Processing Standards

FOA—Field Operating Agency

FOUO—For Official Use Only

FTP—File Transfer Protocol

IA—Information Assurance

IATO—Interim Approval to Operate

I&A—Identification and Authentication

IEEE—Institute of Electrical and Electronics Engineers

ISP—Internet Service Provider

ISSO—Information System Security Officer

ITMRA—Information Technology Management Reform Act

JP—Joint Publication

JTA-AF—Joint Technical Architecture-Air Force

MAC—Mandatory Access Control

MAJCOM—Major Command

NATO—North Atlantic Treaty Organization

NCC—Network Control Center

NCSC—National Computer Security Center

NIPRNET—Non-Secure Internet Protocol Router Network

NIST—National Institute of Standards and Technology

NORAD—North American Aerospace Defense Command

OMB—Office of Management and Budget

OSD—Office of the Secretary of Defense

OSI—Office of Special Investigation

PC—Personal Computer

PCMCIA—Personal Computer Memory Card International Associate

PDA—Personal Digital Assistants

P.L.—Public Law

POC—Point of Contact

RAS—Remote Access Server

SABI—Secret and Below Interoperability

SAF/AA—Administrative Assistant to the Secretary of the Air Force

SAP/SAR—Special Access Program/Special Access Required

SFUG—Security Feature User’s Guide

SIPRNET—Secret Internet Protocol Router Network

SSAA—System Security Authorization Agreement

SSWG—System Security Working Group

TCNO—Time Compliance Network Order

TFM—Trusted Facility Manual

UCM—Unit COMPUSEC Manager

USMCEB—United States Military Communications-Electronic Board

WLAN—Wireless Local Area Network

WM—Workgroup Manager

WWW—World Wide Web

Terms

Accountability—1. Property that allows the ability to identify, verify, and trace system entities as well as changes in their status. Accountability is considered to include authenticity and non-repudiation. 2. (DoD) The obligation imposed by law or lawful order or regulation on an officer or other person for keeping accurate records of property, documents, or funds. The person having this obligation may or may not have actual possession of the property, documents, or funds. Accountability is concerned primarily with records while responsibility is concerned primarily with custody, care, and safekeeping. (JP 1-02)

Accreditation—1. Formal declaration by the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards and controls. 2. (DoD) In computer modeling and simulation, an official determination that a model or simulation is acceptable for a specific purpose. (JP 1-02)

Authenticity—Measure of the confidence that the security features and architecture of an information system accurately mediate and enforce the system security policy.

Category—A grouping of classified or sensitive information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have access approval (e.g., formal access approval). Examples include proprietary, FOUO, Privacy Act, North Atlantic Treaty Organization (NATO), and compartmented information.

Certification—Comprehensive evaluation of the technical and non-technical security features and countermeasures of an information system to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Certifier—Individual responsible for making a technical judgment of the information systems compliance with stated security requirements and requesting approval to operate from the DAA.

Communications and Information Systems Officer (CSO)—At base level, the commander of the communications unit responsible for carrying out communications and information systems responsibilities. At MAJCOM, the person designated by the MAJCOM/CC responsible for overall management of communications and information systems budgeted and funded by that command. When no other office is formally designated as chief information officer (CIO), the CSO ensures compliance with the mandates of the Information Technology Management Reform Act (ITMRA) of 1996.

Computer-Based Security—Security for the information system is provided through the use of automated security features.

Confidentiality—The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls—Prescribed actions taken to maintain the appropriate level of protection for information systems. Controls may validate security activities, detect security incidents and non-conformance, correct deficient security countermeasures, measure the assurance of information system activities, or report incidents. (**NOTE:** There are two divisions of control: management [policy, objectives, and criteria class] and internal [security requirements, mechanisms, and rules]. DoD 7740.1-G, *Department of Defense ADP*

Internal Control Guideline, July 1998, outlines internal controls for information systems.)

Countermeasures—1. The sum of a safeguard and its associated controls. 2. (DoD) That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 1-02)

Designated Approving Authority (DAA)—Official with the authority to formally assume responsibility for operating an information system or network within a specified environment.

Formal Access Approval—Documented approval by a data owner to allow access to a particular category of information.

Information—1. Data derived from observing phenomena and the instructions required to convert that data into meaningful information. (**NOTE:** Includes: operating system information such as system parameter settings, password files, audit data, etc.) 2. (DoD) Facts, data, or instructions in any medium or form. (JP 1-02) 3. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

Information System—1. Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. (**NOTE:** This includes automated information systems.) 2. (DoD) The entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02)

Information Systems Security Officer (ISSO)—Official who manages the COMPUSEC program for an information system assigned to him or her by the UCM; including monitoring information system activities, and ensuring that the information system is operated, maintained, and disposed of according to security policies and practices.

Integrity—Property that allows the preservation of known unaltered states between baseline certifications and allows information, access, and processing services to function according to specified expectations. It is composed of data and system integrity.

Level of Protection—Established safeguards with controls to counter threats and vulnerabilities based on the security requirements. Assures availability, integrity, and confidentiality of the information system.

Nonrepudiation—Method by which the sender of data is provided proof of delivery and the recipient is assured of the sender's identity so that neither can deny having processed the data.

Periods Processing—Processing of various levels of classified and unclassified information at distinctly different times. (**NOTE:** Under periods processing, the information system [operating in dedicated security mode] is purged of all information from one processing period before transitioning to the next when there are different users with different authorizations.)

Safeguards—Protective measures and controls prescribed to meet the security requirements of an information system. (**NOTE:** Safeguards include security features and management constraints from the various security disciplines [i.e., administrative, procedural, physical, personnel, communications, emanations, and computer security] used in concert to provide the requisite level of protection.)

Security Feature—A hardware-, firmware-, or software-controlled access protection to meet the security requirements of I&A; mandatory access control (MAC); discretionary access control (DAC); object reuse; or audit. Security features are a subset of information system security safeguards.

Sensitive Information—Information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. Section 552a (Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept secret in the interest of national defense or foreign policy. (**NOTE:** Systems that are not national security systems, but contain sensitive information are subject to be protected in accordance with the requirements of the Computer Security Act of 1987 [P.L. 100-235].)

Site Certification—Provides assurance that the operational location has implemented the required security measures. This evaluation ensures that the integration and operation of the system is in accordance with the SSAA and a review of the local environment (threats/vulnerabilities).

Stand-Alone System—An information system physically and electronically isolated from all other systems and intended to be used by one user at a time, with no data belonging to other users remaining on the system (e.g., a PC with removable storage media such as a floppy disk).

Standard System—Two or more substantively similar information systems developed for the purpose of fielding multiple copies in support of a mission, within or across MAJCOM or service lines, or DoD-wide.

System Integrity—The attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System Security Policy—Set of laws, rules, and practices that regulate how sensitive and classified information is managed, protected, and distributed by an information system. (**NOTE:** It interprets regulatory [e.g., DoDD 5200.28, AFPD 33-2, AFI 33-202, etc.] and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks, regardless of their sensitivity, criticality, or life-cycle phase, will have a system security policy.)

Tampering—Unauthorized modification that alters the proper functioning of information system security equipment.

Threat—Current and perceived capability, intention, or attack directed to cause denial of service, corruption, compromise, fraud, waste, or abuse to a system.

User—Person or process accessing an information system by direct connections (e.g., via terminals) or indirect connections.

Vulnerability—1. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited. 2. (DoD) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (JP 1-02) 3. (DoD) The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. (JP 1-02)

Workgroup Manager (WM)—A duty supporting a functional community (e.g., workcenters, flights, squadrons, or organizations) and is the first line of help customers contact to resolve problems.

Attachment 2

DOD INFORMATION TECHNOLOGY SECURITY CERTIFICATION AND ACCREDITATION PROCESS (DITSCAP) TASKS

Table A2.1. DITSCAP Tasks.

Tasks	**DoD 8510.1-M Para #**	**Output/Product**
Phase 1: Definition	Chapter 3	
Preparation	C3.3.2.	
1-1. Review documentation	C3.4.1.	**None**
Registration	C3.3.3.	
1-2. Prepare Mission Description and System Identification	C3.4.2.	**SSAA, Section 1**
1-3. Register System	C3.4.3.	**None**
1-4. Prepare Environment & Threat Description	C3.4.4.	**SSAA, Section 2**
1-5. Determine System Security Requirements	C3.4.5.	**SSAA, Section 4**
1-6. Prepare System Security Architecture Description	C3.4.6	**SSAA, Section 3**
1-7. Identify Organization & Resources	C3.4.7	**SSAA, Section 5**
1-8. Tailor DITSCAP/Prepare DITSCAP Plan	C3.4.8.	**SSAA, Section 6**
1-9. Draft the SSAA	C3.4.9	**Completed draft SSAA Document**
Negotiation	C3.3.4.	
1-10. Conduct Certification Requirements Review	C3.4.10.	**None**
1-11. Establish Agreement on Level of Effort and Schedule	C3.4.11.	**None**
1-12. Approve Phase 1 SSAA	C3.4.12.	**Approved SSAA**
Phase II: Verification	Chapter 4	
SSAA Refinement	C4.2.1.	**If necessary, update SSAA**
Systems Integration and Development	C4.2.2.	**None**
Initial Certification Analysis	C4.2.3.	
2-1. System Architecture Analysis	C4.3.2.	**Minimal Security Activity Checklist and Summary Report**

Tasks	DoD 8510.1-M Para #	Output/Product
2-2. Software, Hardware and Firmware Design Analysis	C4.3.3.	**Minimal Security Activity Checklist and Summary Report**
2-3. Network Connection Rule Compliance	C4.3.4.	**Minimal Security Activity Checklist and Summary Report**
2-4. Integrity Analysis of Integrated Products	C4.3.5.	**Minimal Security Activity Checklist and Summary Report**
2-5. Life Cycle Management Analysis	C4.3.6.	**Minimal Security Activity Checklist and Summary Report**
2-6. Security Requirements Validation Procedures	C4.3.7.	**Customized Minimum Security Checklist, Test Plans and Procedures**
2-7. Vulnerability Assessment	C4.3.8.	**Minimal Security Activity Checklist and Vulnerability Assessment Report**
Phase III: Validation	Chapter 5	
SSAA Refinement	C5.2.1.	**If necessary, update SSAA**
Certification Evaluation of Integrated System	C5.2.2	
3-1. Security Test & Evaluation (ST&E)	C5.3.2.	**Minimal Security Activity Checklist and Summary Report**
3-2. Pentration Testing	C5.3.3.	**Minimal Security Activity Checklist and Summary Report**
3-3. TEMPEST and RED-BLACK Verification	C5.3.4.	**Minimal Security Activity Checklist and Summary Report**
3-4. COMSEC Compliance Evaluation	C5.3.5.	**Minimal Security Activity Checklist and Summary Report**
3-5. System Management Analysis	C5.3.6.	**Minimal Security Activity Checklist and Summary Report**
3-6. Site Accreditation Evaluation	C5.3.7.	**Minimal Security Activity Checklist and Summary Report**
3-7. Contingency Plan Evaluation	C5.3.8.	**Minimal Security Activity Checklist and Summary Report**
3-8. Risk Management Review	C5.3.9.	**Minimal Security Activity Checklist and Summary Report**
Recommendation to DAA	C5.2.3.	**Certifier's Recommendation**
Senior Level SSAA Review	Note 1	**Network Risk Assessment Report**
DAA Accreditation Decision (Note 2)	C5.2.4.	**DAA's Accreditation Letter**
Phase IV: Post-accreditation	Chapter 6	
System and Security Operation	C6.2.1.	

Tasks	**DoD 8510.1-M Para #**	**Output/Product**
4-1. SSAA Maintenance	C6.3.2.	**Revised SSAA.**
4-2. Physical, Personnel and Management Control Review	C6.3.3.	**Minimal Security Activity Checklist and Summary Report**
4-3. TEMPEST Evaluation	C6.3.4.	**Summary Report**
4-4. COMSEC Compliance Evaluation	C6.3.5.	**Summary Report**
4-5. Contingency Plan Maintenance	C6.3.6.	**Minimal Security Activity Checklist and Summary Report**
4-6. Configuration Management	C6.3.7.	**Summary Report**
4-7. Risk Management Review	C6.3.8.	**Minimal Security Activity Checklist and Summary Report**
Compliance Validation	C6.2.2.	
4-8. Compliance Validation	C6.3.9.	**Minimal Security Activity Checklist and Summary Report**

NOTES:

1. Systems that do not require a Certificate of Networthiness or Certificate to Operate process still require a Network Risk Assessment performed on them. Stand-alone systems do not require a Network Risk Assessment.
2. DAA's decision to accredit is based on both the Certifier’s recommendation and the Certificate of Networthiness recommendation

Attachment 3

EXAMPLE OF PDA USAGE STATEMENT

MEMORANDUM FOR

FROM: _____ Date: _____

(Rank, Name, Office Symbol)

Subject: Agreement to Use DAA-Approved Privately Owned Personal Digital Assistants (PDA) on the Air Force Enterprise Network

1. My signature below indicates I understand that my privately owned PDA, which is a similar type PDA to the approved government PDAs, has been approved for use by the DAA of the system I am connecting to. In addition to the requirements in AFI 33-202, *Computer Security*, I agree to all the terms, actions, and conditions contained in this letter.

2. I will:

a. Register my PDA with my local equipment custodian for local accountability.

b. Maintain a password on my PDA according to the system security policy.

c. Only use my PDA to process unclassified, non-Privacy Act information.

d. Maintain the same anti-virus software, security standards, and other operational requirements as the government issued PDAs and pay for what is required.

e. Not connect or subscribe to commercial Internet service provider for official E-mail services.

f. Not synchronize information across the Air Force network using a wireless connection.

g. Physically disable any built-in wireless connectivity capability, including infrared.

h. Surrender my PDA (with no reimbursement) if classified information contaminates my PDA.

i. Report any software abnormalities to the ISSO.

j. Not load any software on my PDA without prior authorization.

k. Submit my personal PDA, prior to leaving my current duty assignment, for removal of all sensitive information.

l. Only connect my PDA to the network or system approved by the DAA.

m. Consent to monitoring of my PDA, since it is connected to a system that is subject to being monitoring.

3. I understand my PDA is subject to being audited at anytime to determine if my PDA contains Privacy Act or classified information.

4. I understand that the process for sanitizing sensitive and classified information from my PDA may result in its destruction and I waive any and all claims for reimbursement for any damage or destruction.

5. I understand the Help Desk will assist me with all PC-related problems but repair of my PDA is my responsibility.

6. I understand that if at any time I fail to meet the conditions stated above, I will be required to remove my PDA from connection within the AF protected enclave and submit it for data sanitization.

7. I understand the Air Force does not assume any liability for my PDA, regardless of circumstance. I understand that all data entered on my PDA while performing government business becomes the property of the U.S. Government.

8. Device information:

a. Make & Model: _____

b. Serial number: _____

c. Operating system: _____

d. Installed software: _____

_____

_____

9. I can be contacted at _____.

(phone number and office symbol)

Signature: _____

Signature Block: _____

File:

1 - Maintain original copy with the ISSO

2 - Provide one copy to the individual

Attachment 4

IC 2000-1 TO AFI 33-202, COMPUTER SECURITY

22 JUNE 2000

This instruction implements the computer security (COMPUSEC) portion of Air Force Policy Directive (AFPD) 33-2, *Information Protection*, and establishes Air Force COMPUSEC requirements for information protection to comply with Public Law (P.L.) 100-235, *Computer Security Act of 1987*; Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*; OMB Bulletin 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*; and Department of Defense Directive (DoDD) 5200.28, *Security Requirements for Automated Information Systems (AIS)*, March 21, 1988. You may use extracts from this Air Force instruction (AFI). Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/ITPP), 203 W. Losey Street, Room 1065, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, Recommendation for Change of Publication, with an information copy to HQ AFCA/GCI, 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5222, and HQ Air Force Communications and Information Center (HQ AFCIC/SYI), 1250 Air Force Pentagon, Washington DC 20330-1250. For a glossary of references and supporting information refer to **Attachment 1** and AFDIR 33-303, *Compendium of Communications and Information Technology*. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF REVISIONS

Updates purpose paragraph to include trade name statement. Adds paragraph **3.5.3.** which gives guidance on the use of personal digital assistants (PDA). See the last attachment of the publication, IC 00-1, for the complete IC. A "|" indicates revised material since the last edition.

3.5.3. Guidance on the use of personal digital assistants (PDA):

3.5.3.1. A PDA is an automated information system and therefore is subject to Air Force policy and guidance governing the security and use of a desktop or notebook computer.

3.5.3.2. Use of PDAs (e.g., Palm Pilot® or Cassiopeia® devices) within the Air Force has increased significantly. This family of devices offers personal productivity enhancements, particularly by making certain features of the desktop environment portable (e.g., Microsoft Outlook® contacts, notes, appointments, and E-mail); however, the use of some products and features introduces security risks to information systems and networks.

3.5.3.3. Individuals may use PDAs to:

3.5.3.3.1. Process unclassified information from desktop workstations. This includes the following typical features: schedules, contact information, notes, E-mail, and other items.

3.5.3.3.2. Take notes, save information, or write E-mails, when away from desktop workstations, whether down the hall or out of the country.

3.5.3.3.3. Synchronize information with desktop workstations.

3.5.3.4. Do not use PDAs for the following:

3.5.3.4.1. Do not process or maintain classified information. There are currently no approved methods for clearing (sanitizing) classified information from these devices. If contaminated, security personnel must protect, confiscate, or possibly destroy the affected PDA.

3.5.3.4.2. Do not connect or subscribe to commercial internet service providers (ISP) for official E-mail services (e.g., Palmnet® wireless communications service). The use of commercial ISPs for official business is not allowed due to the high operational risk posed by the possible collection of sensitive information.

3.5.3.4.3. Do not synchronize information across a network using a wireless connection. The configuration required to permit this functionality introduces unacceptable risks into a network--opening firewall ports and sending passwords in the clear. Exceptions to this restriction will be evaluated on a case-by-case basis and require local DAA approval.

3.5.3.5. Software security restrictions described in paragraph **3.4.** apply to these devices.

3.5.3.6. The only authorized connection through a PDA modem is to an official Air Force remote access server (RAS) account protected by an authorized network control center firewall. Do not synchronize the PDA remotely by direct dial-in access to desktops.

3.5.3.7. Do not issue users a PDA until they agree, at a minimum, to the terms outlined in paragraph **3.5.3.**

3.5.3.8. You can find additional security related information on PDAs at the AFCA product evaluation webpage (**http://www.afca.scott.af.mil/prodeval**).

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

CJCSI 6211.02A, Defense Information System Network and Connected Systems, 22 May 1996

CJCSI 6740.01, Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations, 18 September 1996

Information Technology Management Reform Act (ITMRA) of 1996

DoDD 5200.1, DoD Information Security Program, December 13, 1996

DoDD 5200.28, Security Requirements for Automated Information Systems (AISs), March 21, 1988

DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985 (commonly referred to as the Orange Book)

DoD 5220.22-M, National Industrial Security Program Operating Manual, January 1995

DoD 7740.1-G, Department of Defense ADP Internal Control Guideline, July 1998

OMB Circular A-130, Management of Federal Information Resources

OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information

JP 1-02, Department of Defense Dictionary of Military and Associated Terms, 23 March 1994 as amended through 7 December 1998

P.L. 100-235, Computer Security Act of 1987

Title 5 U.S.C. Section 552a (Privacy Act)

AFI 25-201, Support Agreements Procedures

AFI 31-401, Information Security Program Management

AFI 31-601, Industrial Security Program Management

AFI 31-702, System Security Engineering

AFPD 33-2, Information Protection

AFI 33-112, Computer Systems Management

AFI 33-114, Software Management

AFI 33-115V1, Network Management

AFI 33-204, Information Protection Security Awareness, Training, and Education (SATE) Program

AFI 33-205, Information Protection Metrics and Measurements Program

AFI 33-219, Telecommunications Monitoring and Assessment Program (TMAP)

AFMAN 33-223, Identification and Authentication

AFMAN 33-229, Controlled Access Protection (CAP)

DELETE AFMAN 33-270, Command, Control, Communications, and Computer (C4) Systems Security Glossary

AFI 65-201, Management Control

AFDIR 33-303, Compendium of Communications and Information Technology

AFSSI 4100VI, (FOUO) The Air Force Communications Security (COMSEC) Program

AFSSM 5019, Computer Security Users Guide

AFSSI 5020, Remanence Security

AFSSI 5021, Vulnerability and Incident Reporting

AFSSI 5024VI, The Certification and Accreditation (C&A) Process

AFSSI 5024VII, The Certifying Official’s Handbook

AFSSI 5024VIII, The Designated Approving Authority’s Handbook (when published)

AFSSI 5024VIV, Type Accreditation (when published)

AFSSI 5027, Network Security Policy

Abbreviations and Acronyms

ACC	Air Combat Command
ADP	Automated Data Processing
AFCA	Air Force Communications Agency
AFCERT	Air Force Computer Emergency Response Team
AFCIC	Air Force Communications and Information Center
AFI	Air Force Instruction
AFIWC	Air Force Information Warfare Center
AFMAN	Air Force Manual
AIA	Air Intelligence Agency
AFMC	Air Force Materiel Command
AFPD	Air Force Policy Directive
AFSSI	Air Force Systems Security Instruction
AFSSM	Air Force Systems Security Memorandum
ASIM	Automated Security Incident Monitoring
BIOS	Basic Input/Output System
C2	Class 2 (Controlled Access Protection)(a division and class of DoD 5200.28-STD
C&A	Certification and Accreditation
CCB	Configuration Control Board
CINC	Commander-in-Chief
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
COMPUSEC	Computer Security
COMSEC	Communications Security
CSM	Computer Systems Manager
CSO	Communications and Information Systems Officer
CSSO	Computer System Security Officer
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense

DoDD	Department of Defense Directive
DRU	Direct Reporting Unit
DSAWG	DISN Security Accreditation Working Group
FOA	Field Operating Agency
FOUO	For Official Use Only
FTP	File Transfer Protocol
IA	Information Assurance
I&A	Identification and Authentication
IP	Information Protection
ITMRA	Information Technology Management Reform Act
JP	Joint Publication
MAC	Mandatory Access Control
MAJCOM	Major Command
NATO	North Atlantic Treaty Organization
NCC	Network Control Center
NCSC	National Computer Security Center
NIPRNET	Non-Secure Internet Protocol Router Network
OMB	Office of Management and Budget
PC	Personal Computer
P.L.	Public Law
POC	Point of Contact
SABI	Secret and Below Interoperability
SAF	Secretary of the Air Force
SATE	Security Awareness, Training, and Education
SIPRNET	Secret Internet Protocol Router Network
WM	Workgroup Manager
Y2K	Year 2000

Terms

Accountability 1. Property that allows the ability to identify, verify, and trace system entities as well as changes in their status. Accountability is considered to include authenticity and non-repudiation. 2. (DoD) The obligation imposed by law or lawful order or regulation on an officer or other person for keeping accurate records of property, documents, or funds. The person having this obligation may or may not have

actual possession of the property, documents, or funds. Accountability is concerned primarily with records while responsibility is concerned primarily with custody, care, and safekeeping. (JP 1-02)

Accreditation 1. Formal declaration by the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards and controls. 2. (DoD) In computer modeling and simulation, an official determination that a model or simulation is acceptable for a specific purpose. (JP 1-02)

Authenticity Measure of the confidence that the security features and architecture of an information system accurately mediate and enforce the system security policy.

Category A grouping of classified or sensitive information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have access approval (e.g., formal access approval). Examples include proprietary, FOUO, Privacy Act, North Atlantic Treaty Organization (NATO), and compartmented information.

Certification Comprehensive evaluation of the technical and non-technical security features and countermeasures of an information system to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Certifying Official Individual responsible for making a technical judgment of the information systems compliance with stated security requirements and requesting approval to operate from the DAA.

Communications and Information Systems Officer (CSO) At base level, the commander of the communications unit responsible for carrying out communications and information systems responsibilities. At MAJCOM, the person designated by the MAJCOM/CC responsible for overall management of communications and information systems budgeted and funded by that command. When no other office is formally designated as chief information officer (CIO), the CSO ensures compliance with the mandates of the Information Technology Management Reform Act (ITMRA) of 1996.

Computer-Based Security Security for the information system is provided through the use of automated security features.

Computer Systems Manager (CSM) Official with supervisory or management responsibility for an organization, activity, or functional area that owns or operates an information system. They are operationally and administratively responsible for the mission that the information system supports. They are responsible for the security-related functions within their office or facilities. (NOTE: This is not an appointed position. For office automation systems, the office chief or manager is normally the CSM.)

Computer Systems Security Officer (CSSO) Official who manages the COMPUSEC program for an information system assigned to him or her by the CSM; including monitoring information system activities, and ensuring that the information system is operated, maintained, and disposed of according to security policies and practices.

Confidentiality The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls Prescribed actions taken to maintain the appropriate level of protection for information systems. Controls may validate security activities, detect security incidents and non-conformance, correct deficient security countermeasures, measure the assurance of information system activities, or report incidents. (NOTE: There are two divisions of control: management [policy, objectives, and criteria class] and inter-

nal [security requirements, mechanisms, and rules]. DoD 7740.1-G, *Department of Defense ADP Internal Control* Guideline, July 1998, outlines internal controls for information systems.)

Countermeasures 1. The sum of a safeguard and its associated controls. 2. (DoD) That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 1-02)

Designated Approving Authority (DAA) Official with the authority to formally assume responsibility for operating an information system or network within a specified environment.

Formal Access Approval Documented approval by a data owner to allow access to a particular category of information.

Information 1. Data derived from observing phenomena and the instructions required to convert that data into meaningful information. (NOTE: Includes: operating system information such as system parameter settings, password files, audit data, etc.) 2. (DoD) Facts, data, or instructions in any medium or form. (JP 1-02) 3. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

Information System 1. Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. (NOTE: This includes automated information systems.) 2. (DoD) The entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02)

Integrity Property that allows the preservation of known unaltered states between baseline certifications and allows information, access, and processing services to function according to specified expectations. It is composed of data and system integrity.

Level of Protection Established safeguards with controls to counter threats and vulnerabilities based on the security requirements. Assures availability, integrity, and confidentiality of the information system.

Nonrepudiation Method by which the sender of data is provided proof of delivery and the recipient is assured of the sender’s identity so that neither can deny having processed the data.

Periods Processing Processing of various levels of classified and unclassified information at distinctly different times. (NOTE: Under periods processing, the information system [operating in dedicated security mode] is purged of all information from one processing period before transitioning to the next when there are different users with different authorizations.)

Safeguards Protective measures and controls prescribed to meet the security requirements of an information system. (NOTE: Safeguards include security features and management constraints from the various security disciplines [i.e., administrative, procedural, physical, personnel, communications, emanations, and computer security] used in concert to provide the requisite level of protection.)

Security Feature A hardware-, firmware-, or software-controlled access protection to meet the security requirements of I&A; mandatory access control (MAC); discretionary access control (DAC); object reuse; or audit. Security features are a subset of information system security safeguards.

Sensitive Information Information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. Section 552a (Privacy Act), but that has not been specifically

authorized under criteria established by an Executive Order or an act of Congress to be kept secret in the interest of national defense or foreign policy. (NOTE: Systems that are not national security systems, but contain sensitive information are subject to be protected in accordance with the requirements of the Computer Security Act of 1987 [P.L. 100-235].)

Stand-Alone System An information system physically and electronically isolated from all other systems and intended to be used by one user at a time, with no data belonging to other users remaining on the system (e.g., a PC with removable storage media such as a floppy disk).

Standard System Two or more substantively similar information systems developed for the purpose of fielding multiple copies in support of a mission, within or across MAJCOM or service lines, or DoD-wide.

System Integrity The attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System Security Policy Set of laws, rules, and practices that regulate how sensitive and classified information is managed, protected, and distributed by an information system. (NOTE: It interprets regulatory [e.g., DoDD 5200.28, AFPD 33-2, AFI 33-202, etc.] and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks, regardless of their sensitivity, criticality, or life-cycle phase, will have a system security policy.)

Tampering Unauthorized modification that alters the proper functioning of information system security equipment.

Threat Current and perceived capability, intention, or attack directed to cause denial of service, corruption, compromise, fraud, waste, or abuse to a system.

User Person or process accessing an information system by direct connections (e.g., via terminals) or indirect connections.

Vulnerability 1. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited. 2. (DoD) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (JP 1-02) 3. (DoD) The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. (JP 1-02)

Workgroup Manager (WM) A duty supporting a functional community (e.g., workcenters, flights, squadrons, or organizations) and is the first line of help customers contact to resolve problems.

Attachment 5

INTERIM CHANGE 2001-1 TO AFI 33-202, COMPUTER SECURITY

15 February 2001

OPR: HQ AFCA/GCI (MSgt Gorom)

This instruction implements the computer security (COMPUSEC) portion of Air Force Policy Directive (AFPD) 33-2, *Information Protection*, (will become Information Assurance) and establishes Air Force COMPUSEC requirements for information protection to comply with Public Law (P.L.) 100-235, *Computer Security Act of 1987*; Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*; OMB Bulletin 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*; and Department of Defense Directive (DoDD) 5200.28, *Security Requirements for Automated Information Systems (AIS)*, March 21, 1988. You may use extracts from this Air Force instruction (AFI). Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/ITPP), 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, Recommendation for Change of Publication, with an information copy to HQ AFCA/GCI, 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222, and HQ USAF/SCMI, 1250 Air Force Pentagon, Washington DC 20330-1250. For a glossary of references and supporting information refer to **Attachment 1** and AFDIR 33-303, *Compendium of Communications and Information Technology*. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF REVISIONS

This change updates IC 2000-1 (**Attachment 2**). Updates Malicious Logic Protection policy. Updates paragraph **3.13.** which gives guidance on implementing anti-virus software, scanning all incoming traffic and files for viruses, and reporting virus attacks. See the last attachment of the publication, IC 2001-1, for the complete IC. A "|" indicates revised material since the last edition.

2.1. Headquarters United States Air Force Deputy Chief of Staff for Communications and Information (HQ USAF/SC). HQ USAF/SC manages the Air Force COMPUSEC Program.

2.2.1. Reviews, evaluates, and interprets national and DoD COMPUSEC policy and doctrine, and makes recommendations on implementation to HQ USAF/SCM.

2.2.3. Develops, coordinates, publishes, and maintains HQ USAF/SCM-coordinated specialized COMPUSEC publications.

2.2.6. Develops security techniques and procedures with Air Force-wide applicability, coordinates the information with HQ USAF/SCM, and distributes this information to MAJCOMs.

2.11.4.1. Protect system information and resources according to established security policies and procedures.

3.6.1.11. Protect transmission of classified, sensitive, or a combination of classified and sensitive information according to AFI 33-201, *Communications Security (COMSEC).*

3.7. Foreign National Access to Air Force Information Systems. USAF/CVA is responsible for authorizing foreign national access to information systems operated by HQ USAF, DRUs, and Secretary of the Air Force (SAF) functionals. USAF/CVA may further delegate authority to HQ USAF Deputy Chiefs of Staff, and the USAFA Superintendent. Authorizing access to SAF-operated systems is delegated to the SAF assistant secretary level. Delegating authority for these positions shall not occur below the three-star level. MAJCOM commanders (MAJCOM/CC) are responsible for authorizing foreign national access to information systems within their respective commands. Delegating authority shall not occur below the MAJCOM vice commander.

3.13.1.1. Use only anti-virus tools and signature files/datfiles obtained from the AFCERT FTP or DoD Computer Emergency Response Team (CERT) web sites. NCCs will direct configuring (where technically feasible) the signature file update routine to an NCC-controlled site inside the base security perimeter.

3.13.1.1.1. If a waiver is required to use other than DoD anti-virus software, forward requests through your chain of command to HQ AFCA/GCI for approval or disapproval.

3.13.1.2. Activate anti-virus software during AIS use (auto-defend or auto-protect must be enabled to allow a scan when a file is run, opened, copied, moved, created, or downloaded).

3.13.1.3. IA or IPO personnel will check for anti-virus signature files/datfiles updates daily from the AFCERT/DoD CERT sites. Users will schedule ‘Live Updates’ daily to pull down new signature files from the NCC-controlled site or NCC’s site will replicate (if feasible) new signature files to the users as soon as received. A virus scan will be accomplished immediately following an update of a signature file.

3.13.1.4. Establish procedures to rapidly obtain, distribute, and install changes to anti-virus software on all information systems (including network servers).

3.13.3. Scan removable and fixed media:

3.13.3.1. Scan fixed media daily on the core network services listed in AFI 33-115V1, to include all multiuser file servers (e.g., FTP, WWW, network file servers, etc.).

3.13.3.2 The wing DAA (host wing commander) is responsible for establishing the local virus scanning frequency for fixed media on noncore service computing devices (e.g., laptops, desktop computers). The time period between scans will not exceed 7 calendar days. If a local scanning frequency is not established in the host wing's system security policy, scan all fixed media daily.

3.13.3.3. Scan removable media for viruses before each use, which can be automated if anti-virus software is configured properly.

3.13.5. DELETED.

3.13.6. DELETED.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

CJCSI 6211.02A, Defense Information System Network and Connected Systems, 22 May 1996

CJCSI 6740.01, Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations, 18 September 1996

Information Technology Management Reform Act (ITMRA) of 1996

DoDD 5200.1, DoD Information Security Program, December 13, 1996

DoDD 5200.28, Security Requirements for Automated Information Systems (AISs), March 21, 1988

DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985 (commonly referred to as the Orange Book)

DoD 5220.22-M, National Industrial Security Program Operating Manual, January 1995

DoD 7740.1-G, Department of Defense ADP Internal Control Guideline, July 1998

OMB Circular A-130, Management of Federal Information Resources

OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information

JP 1-02, Department of Defense Dictionary of Military and Associated Terms, 23 March 1994 as amended through 7 December 1998

P.L. 100-235, Computer Security Act of 1987

Title 5 U.S.C. Section 552a (Privacy Act)

AFI 25-201, Support Agreements Procedures

AFI 31-401, Information Security Program Management

AFI 31-601, Industrial Security Program Management

AFI 31-702, System Security Engineering

AFPD 33-2, Information Protection

AFI 33-112, Computer Systems Management

AFI 33-114, Software Management

AFI 33-115V1, Network Management

AFI 33-201, Communications Security (COMSEC)

AFI 33-204, Information Protection Security Awareness, Training, and Education (SATE) Program

AFI 33-205, Information Protection Metrics and Measurements Program

AFI 33-219, Telecommunications Monitoring and Assessment Program (TMAP)

AFMAN 33-223, Identification and Authentication

AFMAN 33-229, Controlled Access Protection (CAP)

AFI 65-201, Management Control

AFDIR 33-303, Compendium of Communications and Information Technology

DELETE AFSSI 4100VI, (FOUO) The Air Force Communications Security (COMSEC) Program

DELETE AFSSM 5019, Computer Security Users Guide

AFSSI 5020, Remanence Security (will convert to AFMAN 33-224)

AFSSI 5021, Vulnerability and Incident Reporting (will convert to AFMAN 33-225V2)

AFSSI 5024VI, The Certification and Accreditation (C&A) Process

AFSSI 5024VII, The Certifying Official's Handbook

AFSSI 5024VIII, The Designated Approving Authority's Handbook (when published)

AFSSI 5024VIV, Type Accreditation (when published)

AFSSI 5027, Network Security Policy

Abbreviations and Acronyms

ACC	Air Combat Command
ADP	Automated Data Processing
AFCA	Air Force Communications Agency
AFCERT	Air Force Computer Emergency Response Team
AFI	Air Force Instruction
AFIWC	Air Force Information Warfare Center
AFMAN	Air Force Manual
AIA	Air Intelligence Agency
AFMC	Air Force Materiel Command
AFPD	Air Force Policy Directive
AFSSI	Air Force Systems Security Instruction

AFSSM	Air Force Systems Security Memorandum
ASIM	Automated Security Incident Monitoring
BIOS	Basic Input/Output System
C2	Class 2 (Controlled Access Protection)(a division and class of DoD 5200.28-STD
C&A	Certification and Accreditation
CCB	Configuration Control Board
CINC	Commander-in-Chief
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
COMPUSEC	Computer Security
COMSEC	Communications Security
CSM	Computer Systems Manager
CSO	Communications and Information Systems Officer
CSSO	Computer System Security Officer
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense
DoDD	Department of Defense Directive
DRU	Direct Reporting Unit
DSAWG	DISN Security Accreditation Working Group
FOA	Field Operating Agency
FOUO	For Official Use Only
FTP	File Transfer Protocol
IA	Information Assurance
I&A	Identification and Authentication
IP	Information Protection
ITMRA	Information Technology Management Reform Act
JP	Joint Publication
MAC	Mandatory Access Control
MAJCOM	Major Command

NATO	North Atlantic Treaty Organization
NCC	Network Control Center
NCSC	National Computer Security Center
NIPRNET	Non-Secure Internet Protocol Router Network
OMB	Office of Management and Budget
PC	Personal Computer
P.L.	Public Law
POC	Point of Contact
SABI	Secret and Below Interoperability
SAF	Secretary of the Air Force
SATE	Security Awareness, Training, and Education
SIPRNET	Secret Internet Protocol Router Network
WM	Workgroup Manager
Y2K	Year 2000

Terms

Accountability 1. Property that allows the ability to identify, verify, and trace system entities as well as changes in their status. Accountability is considered to include authenticity and non-repudiation. 2. (DoD) The obligation imposed by law or lawful order or regulation on an officer or other person for keeping accurate records of property, documents, or funds. The person having this obligation may or may not have actual possession of the property, documents, or funds. Accountability is concerned primarily with records while responsibility is concerned primarily with custody, care, and safekeeping. (JP 1-02)

Accreditation 1. Formal declaration by the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards and controls. 2. (DoD) In computer modeling and simulation, an official determination that a model or simulation is acceptable for a specific purpose. (JP 1-02)

Authenticity Measure of the confidence that the security features and architecture of an information system accurately mediate and enforce the system security policy.

Category A grouping of classified or sensitive information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have access approval (e.g., formal access approval). Examples include proprietary, FOUO, Privacy Act, North Atlantic Treaty Organization (NATO), and compartmented information.

Certification Comprehensive evaluation of the technical and non-technical security features and countermeasures of an information system to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Certifying Official Individual responsible for making a technical judgment of the information systems compliance with stated security requirements and requesting approval to operate from the DAA.

Communications and Information Systems Officer (CSO) At base level, the commander of the communications unit responsible for carrying out communications and information systems responsibilities. At MAJCOM, the person designated by the MAJCOM/CC responsible for overall management of communications and information systems budgeted and funded by that command. When no other office is formally designated as chief information officer (CIO), the CSO ensures compliance with the mandates of the Information Technology Management Reform Act (ITMRA) of 1996.

Computer-Based Security Security for the information system is provided through the use of automated security features.

Computer Systems Manager (CSM) Official with supervisory or management responsibility for an organization, activity, or functional area that owns or operates an information system. They are operationally and administratively responsible for the mission that the information system supports. They are responsible for the security-related functions within their office or facilities. (NOTE: This is not an appointed position. For office automation systems, the office chief or manager is normally the CSM.)

Computer Systems Security Officer (CSSO) Official who manages the COMPUSEC program for an information system assigned to him or her by the CSM; including monitoring information system activities, and ensuring that the information system is operated, maintained, and disposed of according to security policies and practices.

Confidentiality The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls Prescribed actions taken to maintain the appropriate level of protection for information systems. Controls may validate security activities, detect security incidents and non-conformance, correct deficient security countermeasures, measure the assurance of information system activities, or report incidents. (NOTE: There are two divisions of control: management [policy, objectives, and criteria class] and internal [security requirements, mechanisms, and rules]. DoD 7740.1-G, *Department of Defense ADP Internal Control* Guideline, July 1998, outlines internal controls for information systems.)

Countermeasures 1. The sum of a safeguard and its associated controls. 2. (DoD) That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 1-02)

Designated Approving Authority (DAA) Official with the authority to formally assume responsibility for operating an information system or network within a specified environment.

Formal Access Approval Documented approval by a data owner to allow access to a particular category of information.

Information 1. Data derived from observing phenomena and the instructions required to convert that data into meaningful information. (NOTE: Includes: operating system information such as system parameter settings, password files, audit data, etc.) 2. (DoD) Facts, data, or instructions in any medium or form. (JP 1-02) 3. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

Information System 1. Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. (NOTE: This includes automated information systems.) 2. (DoD) The

entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02)

Integrity Property that allows the preservation of known unaltered states between baseline certifications and allows information, access, and processing services to function according to specified expectations. It is composed of data and system integrity.

Level of Protection Established safeguards with controls to counter threats and vulnerabilities based on the security requirements. Assures availability, integrity, and confidentiality of the information system.

Nonrepudiation Method by which the sender of data is provided proof of delivery and the recipient is assured of the sender's identity so that neither can deny having processed the data.

Periods Processing Processing of various levels of classified and unclassified information at distinctly different times. (NOTE: Under periods processing, the information system [operating in dedicated security mode] is purged of all information from one processing period before transitioning to the next when there are different users with different authorizations.)

Safeguards Protective measures and controls prescribed to meet the security requirements of an information system. (NOTE: Safeguards include security features and management constraints from the various security disciplines [i.e., administrative, procedural, physical, personnel, communications, emanations, and computer security] used in concert to provide the requisite level of protection.)

Security Feature A hardware-, firmware-, or software-controlled access protection to meet the security requirements of I&A; mandatory access control (MAC); discretionary access control (DAC); object reuse; or audit. Security features are a subset of information system security safeguards.

Sensitive Information Information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. Section 552a (Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept secret in the interest of national defense or foreign policy. (NOTE: Systems that are not national security systems, but contain sensitive information are subject to be protected in accordance with the requirements of the Computer Security Act of 1987 [P.L. 100-235].)

Stand-Alone System An information system physically and electronically isolated from all other systems and intended to be used by one user at a time, with no data belonging to other users remaining on the system (e.g., a PC with removable storage media such as a floppy disk).

Standard System Two or more substantively similar information systems developed for the purpose of fielding multiple copies in support of a mission, within or across MAJCOM or service lines, or DoD-wide.

System Integrity The attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System Security Policy Set of laws, rules, and practices that regulate how sensitive and classified information is managed, protected, and distributed by an information system. (NOTE: It interprets regulatory [e.g., DoDD 5200.28, AFPD 33-2, AFI 33-202, etc.] and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks, regardless of their sensitivity, criticality, or life-cycle phase, will have a system security policy.)

Tampering Unauthorized modification that alters the proper functioning of information system security equipment.

Threat Current and perceived capability, intention, or attack directed to cause denial of service, corruption, compromise, fraud, waste, or abuse to a system.

User Person or process accessing an information system by direct connections (e.g., via terminals) or indirect connections.

Vulnerability 1. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited. 2. (DoD) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (JP 1-02) 3. (DoD) The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. (JP 1-02)

Workgroup Manager (WM) A duty supporting a functional community (e.g., workcenters, flights, squadrons, or organizations) and is the first line of help customers contact to resolve problems.

Attachment 6

INTERIM CHANGE 2001-2 TO AFI 33-202, COMPUTER SECURITY

30 AUGUST 2001

This instruction implements the computer security (COMPUSEC) portion of Air Force Policy Directive (AFPD) 33-2, *Information Protection*, (will become Information Assurance) and establishes Air Force COMPUSEC requirements for information protection to comply with Public Law (P.L.) 100-235, *Computer Security Act of 1987*; Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*; OMB Bulletin 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*; Department of Defense Directive (DoDD) 5200.28, *Security Requirements for Automated Information Systems (AIS)*, March 21, 1988; DoDI 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*, December 30, 1997; and Department of Defense (DoD) 8510.1-M, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, July 31, 2000. The Uniform Code of Military Justice applies to personnel who violate the specific prohibitions and requirements of this instruction. You may use extracts from this Air Force instruction (AFI). Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/ITPP), 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, Recommendation for Change of Publication, with an information copy to HQ AFCA/GCI, 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222, and HQ USAF/SCMI, 1250 Air Force Pentagon, Washington DC 20330-1250. Send supplements to this publication to HQ AFCA/GCI for review, coordination, and approval prior to publication. For a glossary of references and supporting information refer to **Attachment 1** and AFDIR 33-303, *Compendium of Communications and Information Technology*. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF REVISIONS

This change updates IC 2000-1 (**Attachment 4**) and IC 2001-1 (**Attachment 5**). It includes reference to an additional DoD instruction and manual. Updates and clarifies policy for foreign national access. Adds a statement that personally owned information systems will be confiscated if contaminated with classified information. Adds policy on wireless local area network (WLAN) and additional requirements for PDA usage, including an example of a PDA usage statement (**Attachment 3**). Adds **Chapter 4**, which talks about the certification and accreditation (C&A) process. References to AFSSI 5024 were changed to reflect this document and the term Computer System Security Officer is changed to Information System Security Officer (ISSO). Adds a new attachment (**Attachment 2**) that lists the C&A task. Updates the title to AFSSI 5021 and changes AFCERT Advisories to Time Compliance Network Order (TCNO). Updates assignment of the Designated Approving Authority (DAA). Updates the training requirements for users and unit COMPUSEC managers and references, abbreviations and acronyms, and terms. See the last attachment of the publication (**Attachment 6**, IC 2001-2) for the complete IC. A "|" indicates revised material since the last edition.

1.5. DELETED.

1.5.1. DELETED.

1.5.1.1. DELETED.

1.5.1.2. DELETED.

1.5.1.3. DELETED.

1.5.2. DELETED.

1.5.3. DELETED.

1.5.3.1. DELETED.

1.5.3.2. DELETED.

1.5.3.3. DELETED.

1.5.3.4. DELETED.

1.5.4. DELETED.

2.5.3.2. Develops a certification and accreditation (C&A) plan and documents it in the System Security Authorization Agreement (SSAA).

2.5.3.3. Certifies and accredits information systems according to **Chapter 4** of this AFI and performs duties identified for the Program Manager.

2.5.3.8. Ensures operating agencies receive copies of the SSAA documentation.

2.5.3.9. Ensures the SSAA documentation defines security procedures for system users, administrators, and maintainers.

2.5.3.11. Determines the sensitivity level of the information and the criticality of information system resources and information.

2.5.3.12. Plans and programs budgetary, manpower, and training support for the implementation and continuation of the COMPUSEC program to include improvements to security.

2.5.3.13. Ensures the Designated Approving Authority (DAA) and users participate throughout the system development cycle in security analyses performed in conjunction with all design and specification reviews.

2.5.3.14. Is responsible for ensuring the appropriate coordination and review of all decisions concerning security trade-off and changes in requirements with the Certifier, system developers, users, and the DAA (see AFI 31-702).

2.5.3.15. Is the focal point for security system engineering during the system requirements definition, design, implementation, and testing phases of the program.

2.5.3.16. Responsible for ensuring security measures are implemented to adequately satisfy the security specification and any residual risks are identified.

2.6. Other Agencies Acquiring or Developing Information Systems or Software. Assume single manager responsibilities (paragraph **2.5.3.**) when they develop systems or software outside a program management office structure.

2.7.2. As necessary, appoints a DAA representative to deal with the day-to-day issues of accrediting information systems according to **Chapter 4**.

2.7.3. Identifies Information Systems Security Officers (ISSO) for all information systems under the DAA's jurisdiction.

2.7.5. Appoints a certifier to accomplish information system certification. Makes sure this individual possesses the technical expertise on the information system being certified and on the security mechanisms in use.

2.7.6. Makes appropriate decisions to balance security requirements, mission, and resources against the defined or perceived threat.

2.7.7. Ensures resources are available to support the certification and security countermeasures.

2.7.8. Formally assumes responsibility for the secure operation of the information system to operate in a specific environment.

2.7.9. Ensures the security policy is developed and certification goals are clearly defined.

2.7.10. Is responsible for approving security requirements documents, memorandums of agreement, and deviations from security policy.

2.7.11. Accredits all information systems and applications under their authority prior to their operation.

2.8. Certifier:

2.8.1. Coordinates certification activities and places all documentation into the SSAA for presentation to the DAA.

2.8.4. Is the formal certifying authority for the system and ensures the SSAA appropriately addresses the system security policy objectives.

2.8.5. Validates and assesses the risks associated with operating the system.

2.9.1.5. DELETED.

2.9.1.7. Designates a focal point to track and ensure MAJCOM compliance with C&A requirements for both classified and unclassified systems. The MAJCOM focal point acts as the point of contact (POC) to the Defense Information Systems Agency (DISA) for the command regarding the SSAA documentation.

2.10.1.4. Provides accreditation guidance and assistance.

2.10.1.7. DELETED.

2.11. Organizations. Commanders appoint in writing a unit COMPUSEC manager to oversee their COMPUSEC program. Unless required by the MAJCOM or wing, official designation of ISSOs is at the discretion of the unit COMPUSEC manager. If the ISSO positions are not assigned, the ISSO responsibilities reside with the unit COMPUSEC manager.

2.11.1.4. Provides a copy of appointment letter to the wing IA office.

2.11.1.5. Ensures ISSOs are assigned to functional systems or on a system-by-system basis.

2.11.1.6. Provides C&A information to the wing IA office for appropriate tracking.

2.11.2. DELETED.

2.11.2.1. DELETED.

2.11.2.2. DELETED.

2.11.2.3. DELETED.

2.11.2.4. DELETED.

2.11.2.5. DELETED.

2.11.2.6. DELETED.

2.11.2.7. DELETED.

2.11.2.8. DELETED.

2.11.2.9. DELETED.

2.11.2.10. DELETED.

2.11.3. ISSO. Workgroup managers (WM) may perform some or all of the duties listed below:

2.11.3.2. Ensures procedures are in place for users to notify the ISSO or alternate if problems arise during critical or classified processing.

2.11.3.5. Performs an initial evaluation of each vulnerability or incident and begins corrective or protective measures and reports according to AFSSI 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting* (will become AFMAN 33-225, Volumes 1 and 2).

2.11.3.7. Ensures all network and system administrators are taking aggressive action to implement TCNO and comply with the vulnerability and incident reporting procedures according to AFSSI 5021 (will become AFMAN 33-225, Volumes 1 and 2).

2.11.3.10. Maintains the accreditation according to **Chapter 4**.

2.11.3.11. DELETED.

2.11.3.12. Ensures organizations do not use shareware or public domain software until approved for use by the DAA. The ISSO ensures the software is free of viruses, hidden defects, and obvious copyright infringements. The ISSO or WM perform testing.

2.11.3.13. Monitors information system activities to ensure system integrity; establishes reaction and maintenance controls for the facility; and performs system access or revocation tasks.

2.11.3.14. Continually identifies threats, deficiencies, and associated countermeasures.

2.11.3.15. Reports system security incidents, vulnerabilities, and virus attacks according to AFSSI 5021 (will convert to AFMAN 33-225, Volume 2).

2.11.3.16. Establishes restrictions on shared usage of programs or files.

2.11.3.17. Ensures site certification is obtained before operational use.

2.11.3.18. Ensures each information system operates within the constraints of the system security policy and network security policy.

2.11.3.19. Ensures measures exist to control access to information systems based on users' validated clearances, access approval for categories, and need to know.

2.11.3.20. Maintains information systems processing sensitive, classified, and critical information according to configuration management controls, and provides security guidance to the established configuration control board (CCB).

2.11.3.21. Identifies information ownership for each multi-user information system to include accountability, access rights, and special handling requirements.

3.1.1. Prior to operating, certify and accredit all information systems according to **Chapter 4**.

3.1.4. DELETED.

3.2.1. The host wing commander is the DAA for the base-wide area or metropolitan area network to include the core services (backbone [to include routers, switches, and hubs], boundary protection, E-mail, NT server farms), network infrastructure (to include workstations, printers and network devices, etc. regardless of ownership), and standalone systems for each installation; this authority will not be delegated.

3.2.1.1. DELETED.

3.2.1.2. The wing commander may appoint a DAA representative at each geographically separated unit (GSU) if the GSU's network boundary protection (i.e., firewall, intrusion detection) is provided by the host network control center. If the GSU is responsible for its own boundary protection the wing commander may delegate DAA authority to the ranking officer at the GSU. In this instance, further delegation is prohibited.

3.2.2. MAJCOM, FOA, DRU, and tenant unit commanders are DAAs for unique systems and networks they own and operate. This authority may be delegated to the 2-letter/deputy level MAJCOM functional office. This also applies to MAJCOM consolidated systems spread throughout their respective bases. MAJCOMs that expand their accreditation boundary to include all of their bases are the DAA for all of their bases. Further delegation is prohibited.

3.2.2.1. DELETED.

3.2.2.2. DELETED.

3.2.3. The Air Force Chief Information Officer (AF-CIO) is the responsible official for Air Force owned and operated functional systems in the Air Force enterprise. The Air Staff 2-letter director levels have DAA authority for their appropriate functional systems. This authority maybe delegated to their 3-letter director level. If the authority is delegated, they are the DAA for those functional systems from cradle to grave. For example, for Integrated Logistics Systems-Supply, the HQ USAF/IL could delegate DAA authority to HQ USAF/ILS. Further delegation is prohibited.

3.2.4. The Administrative Assistant to the Secretary of the Air Force (SAF/AA) is the DAA for all information systems, regardless of classification, used inside Air Force Special Access Program/Special Access Required (SAP/SAR) programs and program facilities. This authority may be delegated to Air Staff offices responsible for the security of specific SAP/SAR programs. Further delegation may occur only with SAF/AA approval.

3.3.2.3. Select a suitable product, then test and certify its security features according to **Chapter 4**. Certification must validate claims that the security features meet Air Force and DoD security policy or that additional countermeasures are required.

3.4.1. Certify all software prior to installation and use on an operational accredited system. Follow the certification process outlined in **Chapter 4** and ensure DAA approval is granted. (*NOTE:* Freeware, public domain software, and shareware originating from questionable or unknown sources, [e.g., non-DoD bulletin boards or World Wide Web sites, etc.] are much more susceptible to malicious logic and may violate the system security policy. Base use of such software on operational need.)

3.5.1.5.1. Disable ActiveX and Java features when visiting untrusted sites (non-.gov or -.mil sites). When mission accomplishment necessitates the need to enable these features, obtain DAA approval and update the SSAA.

3.5.1.7. DELETED.

3.5.3.9. The following applies to handling and controlling of PDAs:

3.5.3.9.1. Disable auto sync on the desktop application menu until needed. Once the PDA and computer have synced up, turn off the auto-sync.

3.5.3.9.2. Password protect PDAs according to AFMAN 33-223, if technically possible. If the PDA is technically unable to use a password, increase physical access controls to prevent unauthorized access.

3.5.3.9.3. Disable infrared (IR) port beaming capability. If the IR port is unable to be disabled, cover the IR port with a visor or similar object (i.e., tape).

3.5.3.9.4. Turn off PDAs when not in use.

3.5.3.10. Include PDAs in the SSAA for the network. Ensure vulnerabilities associated with the PDAs are included in the threat and vulnerability assessment. Reflect the handling, controlling and usage of PDAs in the network security policy.

3.5.3.11. Connecting privately owned PDAs to the Air Force network is strongly discouraged. If individuals have a requirement to use a PDA on the Air Force network, they must request issuance of a government-owned PDA. Privately owned PDAs will not be connected to the Air Force network without sufficient justification and the DAA approval. Justification must include mission requirements, government availability, and rationale of how duty position will be enhanced. Include handling of privately owned PDAs and software in the SSAA. Individuals must sign a PDA usage statement (**Attachment 3**) agreeing to the terms outlined in this instruction.

3.5.3.12. Do not use PDAs in classified environments because of their infrared and similar recording capabilities. PDAs (includes privately owned) contaminated with classified information will be confiscated and possibly destroyed, since there is currently no means to sanitize the PDA.

3.6.1.6. Limit access to privileged programs (i.e., operating system, system parameter and configuration files, and databases), utilities (i.e., assemblers, debuggers, maintenance utilities), and security-relevant programs/data files (i.e., security monitor, password files, and audit files) to authorized personnel (i.e., system administrator and ISSO).

3.7. Requirements for Foreign National Access to Unclassified But Sensitive Internet Protocol Router Network (NIPRNet).

3.7.1. Requests to grant foreign national access to information systems and networks by foreign governments, allied and coalition organizations are handled as follows: the wing commander sends the request to

the MAJCOM/CC who verifies the need, then forwards it to HQ USAF/SC for Air Force approval; it is then validated by the Joint Staff/J6 and approved/disapproved by the Office of the Secretary of Defense (OSD).

3.7.1.1. DELETED.

3.7.1.2. DELETED.

3.7.1.3. DELETED.

3.7.1.4. DELETED.

3.7.2. Provide the following information in the request to OSD for foreign national access approval:

3.7.2.1. Mission Statement and description of current environment.

3.7.2.2. Organizations involved and POCs.

3.7.2.3. Type of connectivity required (e.g., HTTP, Simple Mail Transfer Protocol, FTP, etc.)

3.7.2.4. What type of information and how often information will be transmitted.

3.7.2.5. Verification that foreign disclosure has been made by the appropriate DAA.

3.7.3. Request to grant foreign national access to information systems and networks to the following category of individuals is based on the access needed and is approved by the Approving Authority stated in **Table 3.1.** The Approving Authority approves access for the following individuals:

3.7.3.1. Assigned to the Defense Personnel Exchange Program.

3.7.3.2. Assigned to the Cooperative Program.

3.7.3.3. Employed Overseas by the U.S. Government under Status of Forces Agreement.

3.7.3.4. Assigned to CONUS based North American Aerospace Defense Command (NORAD).

3.7.3.5. Employed CONUS by the U.S. Government.

3.7.3.6. Foreign Military personnel temporarily assigned to Air Force-sponsored training programs (i.e., Air Force Academy, Air Education and Training Command (AETC) training courses, medical students, etc.)

3.7.3.7. Employed overseas by foreign national contractor.

3.7.3.8. Individuals assigned to the Foreign Liaison Officer Program.

Table 3.1. Approving Authority for Foreign National Access.

Access Needed	Approving Authority
E-mail (1)	Local Host Wing DAA
Stand alone and networks within a local enclave	
NIPRNet (2)	MAJCOM CC/CV
Functional System Access	DAA of System

NOTES:

1. E-mail accounts of foreign nationals must identify the individuals as foreign personnel to include position assigned. Example: lastname, firstname, rank, country of origin-assignment, office symbol; Doe, John, WG CDR, UK-FLO, CENTAF/A6.

2. Does not constitute full NIPRNet access, controls must be in place to ensure only authorized sites are accessed.

3.7.4. Once approved, grant network access (to include (NIPRNet)) to these individuals and limit access to the extent necessary to perform assigned duties. *NOTE:* Approval to access the NIPRNet or other networks by foreign personnel does not equate to authority to exchange data or access systems located on that network. The system DAA grants access to the information systems and Designated release/disclosure authority grants access to information.

3.7.4.1. DELETED.

3.7.5. Before authorizing foreign national access to information supervisors will:

3.7.5.1. Identify specific information system access requirements for the position.

3.7.5.2. Work with the unit COMPUSEC manager (UCM) and ISSO to implement necessary controls to assure that only authorized information systems are accessible by approved personnel, as defined by the foreign disclosure officer.

3.7.5.3. Ensure that access to any unclassified information system or web site containing information that is controlled under the Arms Export Control Act, Privacy Act, and exemptions to the Freedom of Information Act is approved by the system DAA/webmaster and the local foreign disclosure officer.

3.7.5.4. Ensures security measures employed adhere to information assurance policy.

3.7.6. In addition, foreign nationals who have access to specific information contain within a functional system, the local DAA will ensure:

3.7.6.1. The information is properly processed for disclosure.

3.7.6.2. The local foreign disclosure officer validates that these requirements fall within the limits of the disclosure authority approved for the position.

3.7.6.3. The SSAA for the system is updated to reflect foreign national access.

3.7.7. Foreign Nationals who are permanent residents of the U.S have the same status as U.S. citizens and are exempt from these procedures.

3.10.4. Personally Owned. Do not use personally owned information systems (i.e., hardware or software) to process classified information. Using personally owned hardware and software for government work is strongly discouraged; however, it may be used for processing unclassified and sensitive information with DAA approval (see AFI 33-112, *Computer Systems Management*; and AFI 33-114, *Software Management*). (*NOTE:* Document blanket approvals for the purpose of telecommuting in a local operating instruction.) Approved personally owned information systems contaminated with classified information will be confiscated. Base approval on the following requirements:

3.12. Requirements for Foreign National Access to SIPRNet. Request Joint Staff/J6 validation and OSD approval in order to connect to DISN-SIPRNET (use the same process listed in paragraph **3.7.1.** to obtain approval). The request must include items identified in the draft DISA Connection Approval Process (i.e., mission statement, organizations involved, POC, brief description of current environment to include topology, consent-to-monitor statement, etc.). The technical solution must include a high assurance guard in United States-controlled space to protect United States-only information and information systems. The Certifier must submit the SSAA to DISA and present the technical solution to the DISN Security Accreditation Working Group (DSAWG). If approved, the DSAWG advises the sponsoring Commander-in-Chief (CINC), Air Force and DISA, in writing, so DISA can grant the approval to connect.

3.13.8. Include virus prevention, detection, eradication, and reporting procedures in user training.

3.14. Training. License network users according to AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*. The wing IA office trains UCMs on this instruction, identification and authentication, remanence security, vulnerabilities and incidents reporting, etc.

3.17. Wireless Local Area Networks (WLAN).

3.17.1. Apply the following security requirements to wireless solutions. WLANs are susceptible to interference and are easily jammed:

3.17.2. All existing WLANs operating prior to 1 June 2001 may continue to operate; however, the responsible DAA must provide a migration plan to ensure the systems meet the requirements by 1 January 2003. Air Force unclassified networks will be enabled for hardware token, certificate-based access controls no later than October 2002.

3.17.2.1. WLAN solutions must meet the same C&A requirements as wired LAN solutions, according to **Chapter 4**. Program Management Offices must consider these requirements during the development of a WLAN solution.

3.17.2.2. Engineer WLAN solutions to preclude backdoors into the Air Force enterprise network.

3.17.2.3. Configure wireless equipment for appropriate local area network (LAN) security options. Commercial-off-the-shelf products typically arrive with factory default settings, which may not offer LAN security.

3.17.2.4. Use encryption standards to protect information accordingly. Encrypt all radio frequency wireless networks according to AFI 33-201. Comply with AFSSI 7010, *(S) Emission Security Assessment (U)* (will convert to AFMAN 33-214V1), for WLANs.

3.17.2.5. Use National Institute of Standards and Technology (NIST) standard, Federal Information Processing Standards (FIPS) Pub 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001, Triple data encryption standard encryption, or the new NIST advanced encryption standard (expect FIPS publication April-June 2001) for encryption of sensitive information.

3.17.2.6. Ensure that a user cannot enter a WLAN without strong authentication. As a minimum, strong authentication should include an extended service set identifier and mandatory access control (MAC) address identification with an integrity lock.

3.17.2.7. Use Institute of Electrical & Electronics Engineers (IEEE) 802.11 standard for WLANs using the Direct Sequence Spread Spectrum (less susceptible to jamming, better throughput) or Frequency Hopping Spread Spectrum (more difficult to intercept) standards.

3.17.2.8. Coordinate use of any wireless device, including commercial nonlicensed devices, with the local Air Force frequency manager. Coordinate any use in foreign nations with the United States Military Communications-Electronic Board (USMCEB) on a system specific basis, for spectrum supportability determination. Supportability alone will not authorize approval to operate the system. A frequency assignment is required from the host nation prior to equipment usage. The local frequency manager can assist with processing a spectrum supportability determination from the USMCEB and processing a frequency assignment request from the host nation. Use of wireless devices may not be approved for use in another country, since each country allocates its frequency resources differently. This can also be an issue in the CONUS. Also, if a nonlicensed WLAN interferes with licensed equipment, i.e., medical equipment, Federal Communications Commission regulations require the WLAN to shut down. *NOTE*: If a private WLAN interferes with a federal WLAN, the federal WLAN must accept the interference. If a federal WLAN interferes with a private WLAN the federal WLAN must shut down. See AFI 33-118, *Radio Frequency Spectrum Management,* for more information.

3.17.2.9. Certify all wireless devices for spectrum supportability prior to obligating funds according to AFI 33-118.

3.17.2.10. Use replaceable WLAN radios (Personal Computer Memory Card International Associate [PCMCIA] or PC cards) in all devices attached to WLAN.

3.17.2.11. Comply with AFMAN 33-120, *Radio Frequency (RF) Spectrum Management,* which prohibits the use of WLANs for critical or command and control systems.

3.17.2.12. Ensure continuity of operations plans include using alternative manual procedures in case of automated system failure.

3.17.2.13. Conduct a risk analysis to determine the information intercept and monitoring vulnerabilities (e.g., electronic emanations, emission security [EMSEC], etc.), prior to implementing WLANs. Review all EMSEC assessments on all classified systems within the same building or within 20 meters of any components of the WLAN before beginning engineering, installation, or ordering the LAN.

3.17.2.14. Ensure that the administrators have the capability to audit or monitor the WLAN to detect intrusions. Intrusions are not always detected immediately. If logs are not available, it will be difficult to troubleshoot unauthorized access.

3.17.2.15. Remotely configure access points on the wired side of the WLAN configuration. This will prevent an intrusion on the wireless side from intercepting configuration information and changing the WLAN settings.

3.17.2.16. Simple Network Management Protocol is often used to remotely configure an access point. Change default community strings to prevent unauthorized configuration (read and write privileges to access point).

3.17.2.17. Ensure unused protocols are filtered at the access point. This will enhance the security and efficiency of the WLAN.

3.17.3. Consider the following characteristics and parameters of wireless solutions prior to the use of any wireless solution:

3.17.3.1. Wireless solutions may create backdoors into Air Force LANs. If a device receives information via a wireless technology and that device allows that information to be placed directly into the LAN via cable at the workstation level, then all perimeter and host-based security devices may have been bypassed.

3.17.3.2. When utilizing a wireless LAN solution the LAN card's unique numeric identifier (MAC address) can be copied electronically (spoofed). It is important to ensure strong authentication, i.e., PKI or FIPS compliant device or SECNET 11. The user cannot rely totally on MAC address resolution as the only means for authentication.

3.17.3.3. Wireless LANs are susceptible to interference, interception, and are easily jammed. Clearly define standards and publish WLAN security policies in the network security policy.

Chapter 4

CERTIFICATION AND ACCREDITATION

4.1. Background. The Computer Security Act of 1987 established the requirement for every information system to be certified and accredited.

4.1.1. For several years, AFSSI 5024 was the guidance by which Air Force information systems were certified and accredited. In order to fall in line with the other DoD services, the Air Force is transitioning to the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). DoDI 5200.40, *Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)* (will become DoDI 8510.1), implements guidance to standardize the Certification and Accreditation (C&A) process throughout the DoD. DoD 8510.1-M, *Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, is the application manual that explains the step-by-step process on how to accomplish C&A using the DITSCAP. See **Table 4.1.** for a cross-reference from old terms to the new terms.

4.1.2. Effective 1 April 2001, use DITSCAP to certify and accredit new systems or existing systems that have not been previously certified and accredited. For those systems that are actively working the C&A process (prior to 1 April 2001 and in AFSSI 5024 Phase II or higher), may complete the C&A process using AFSSI 5024. Systems in spiral development will transition to DITSCAP no later than 1 April 2002. Systems that have completed a C&A process according to AFSSI 5024, will transition to DITSCAP when recertification or reaccreditation is required.

Table 4.1. Cross-Reference of Old Terms with the New Terms

Old Term	New Term
System Program Office (SPO)	Program Manager
Single Manager (SM)	
Certifying Official	Certifier
Computer Systems Security Officer (CSSO)	Information Systems Security Officer (ISSO)
Full Accreditation	Accreditation
Interim Accreditation	Interim Approval to Operate (IATO)
C&A Package	System Security Authorization Agreement (SSAA)

4.2. Roles and Responsibilities. Key roles and responsibilities in the DITSCAP process include the DAA, Certifier, Program Manager, User Representative, and the ISSO. Some of these key roles are explained in **Chapter 2** of this instruction and additional information is contained in Chapter 8 of DoD 8510.1-M. There are numerous other personnel and agencies that support the C&A tasks. The number of participating organizations and their assignments will differ between programs based on the guidance set forth by the DAA, availability of resources, level of effort for certification, the security requirements, as well as the sensitivity and criticality of the system. It is equally important to identify their roles and responsibilities early on and include this information in the SSAA. In addition, the following information is provided as an overview of *typical* assignments of responsibilities to the various participants.

4.2.1. Designated Approving Authority (DAA). This person has the largest effect on the scope of C&A work. See paragraph **2.7.** for the DAA roles and responsibilities.

4.2.1.1. DAA Representative. To ease the burden of dealing with the day-to-day issues of accrediting information systems, the DAA may appoint a representative to perform many of the duties. The DAA Representative remains actively involved in certification tasks and keeps the DAA informed of major issues. They identify, address, and coordinate security accreditation issues with the DAA. A direct link must exist between the DAA Representative and the DAA. However, the DAA, not the DAA Representative, makes the accreditation decision.

4.2.1.2. DAA Liability. It is imperative that the DAA understands the legal ramifications of signing the accreditation document. They ensure that the appropriate security measures, documentation, and the C&A process are implemented and maintained throughout the life cycle of the information systems.

4.2.1.2.1. When granting approval to operate, the DAA accepts the ultimate responsibility for its operation and officially declares:

4.2.1.2.1.1. The specified system adequately protects the information or resources.

4.2.1.2.1.2. Acceptance of the residual risks involved in operating the system.

4.2.1.2.2. Maintain sufficient documentation to support the DAA's accreditation decision as well as to verify the implementation and operational maintenance of designated security measures or system safeguards.

4.2.1.3. DAA Training. DAAs need to familiarize themselves with responsibilities, directives, regulations, and laws applicable to C&A, before initiating the C&A process.

4.2.2. Certifier. The Certifier is crucial to the success of the entire C&A effort. See paragraph 2.8 for the Certifier's roles and responsibilities.

4.2.3. Program Manager. The program manager coordinates all aspects of the system from initial concept, through development, to implementation, and system maintenance. The program manager performs roles of the Single Manager listed in paragraph **2.5.3.**

4.2.4. User Representative. The user representative is the liaison for the user community throughout the life cycle of the system. The user representative defines the system's operations and functional requirements and is responsible for ensuring that the user's operational interests are maintained throughout system development, modification, integration, acquisition, and deployment. See DoD 8510.1-M, Chapter 8 for additional roles and responsibilities.

4.2.5. Information System Security Officer (ISSO). The ISSO assists in the development of the system security policy and ensures compliance on a day-to-day basis. Their most important role is during the Post-Accreditation Phase where they ensure the security posture of the system and the accreditation is maintained. They also perform roles identified in paragraph **2.11.3.**

4.2.6. Other Roles.

4.2.6.1. Certification Team. Working for the Certifier, the Certification Team accomplishes C&A according to the DITSCAP. Team members evaluate the technical and nontechnical features of the system to determine the level of protection provided and document their findings. Each member is responsible to the Certifier for the evaluations they perform and the documentation they submit. The composition and size of the team will depend on the size and complexity of the system. Compose the team of members that have composite expertise in the whole span of activities requirement and who are independent of the system developers or project manager.

4.2.6.2. System Security Working Group (SSWG). This group directs security tasks, and identifies and resolves security-related issues throughout the system life cycle according to AFI 31-702. The group provides continuity among the system security policy, the system design, and the security engineering approach.

4.3. System Security Authorization Agreement (SSAA). The SSAA is the depository of evidence showing that the system meets the system security policy, all certification tasks are properly completed, the system is approved to operate, and a plan for maintaining the accreditation exists.

4.3.1. SSAA Outline. Use the SSAA outline in DoD 8510.1-M, Appendix 1. List all items in the SSAA outline. For those items that do not apply, list the outline number, the detailed description, and then N/A. Refer to Table A2.1 for a chart that references the task with the specific paragraph in DoD 8510.1-M.

4.3.1.1. In addition to Appendices A through R required by DoD 8510.1-M, the Air Force requires the additional mandatory appendices:

4.3.1.1.1. Appendix S - Certificate of Networthiness/Networthiness Recommendation.

4.3.1.1.2. Appendix T - Minimal Security Activity Checklists.

4.3.1.1.3. Appendix U - Network Vulnerability Assessment Reports.

4.3.1.1.4. Appendix V - Trusted Facility Manual (TFM).

4.3.1.1.5. Appendix W - Security Features User’s Guide (SFUG).

4.3.1.2. MAJCOMs may require additional appendices to meet specific needs. Include all documentation that is relevant to the C&A process.

4.3.2. Automated Tools. DISA provides an automated tool to aid in the preparation of the SSAA, which can be downloaded from **https://www.afca.scott.af.mil/ip/compusec/cna/cna.htm**.

4.3.3. Accreditation Boundaries.

4.3.3.1. Networks. When accrediting a network, it is not necessary to certify individual workstations on the system. Include the workstations in the network description, as long as all of the workstations contain similar software and hardware.

4.3.3.2. Systems. A system can be as small as a stand-alone workstation or as large as a complete network, with servers, router, hubs, workstations, etc. Software requires a platform (hardware) in order to operate. Certify the environment in which the software is operating. The software and hardware are accredited together as a system.

4.3.4. Security Test and Evaluation (ST&E). Use only JTA-AF approved software during ST&E.

4.4. Accreditation/Interim Approval to Operate (IATO). The decision to grant an accreditation, IATO, or disapproval is based on both the Certifier's recommendation and Certificate of Networthiness recommendation.

4.4.1. Accreditation. Accreditation is the formal declaration by the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards and controls; not to exceed 3 years. *NOTE:* Only an IATO can be issued if a Certificate of Networthiness is issued with conditions.

4.4.2. Interim Approval to Operate (IATO). The system does not meet the requirements as stated in the SSAA. Mission criticality mandates the system become operational and no other capability exists to adequately perform the mission. The IATO is a temporary approval issued for the minimal period of time necessary to meet all SSAA requirements (to achieve accreditation); not to exceed 1 year.

4.5. Site Certification.

4.5.1. Conduct site certification for systems that have a Certificate of Networthiness, a Certificate to Operate, or have a type accreditation signed by the functional DAA. The system still requires a site certification upon its arrival at the site.

4.5.2. Site certification provides assurance that the operational location has implemented the required security measures. This evaluation ensures that the integration and operation of the system in accordance with its certified design and operational concept pose an acceptable risk to the information being processed.

4.5.3. Site certification consists of:

4.5.3.1. Conducting the Site Accreditation Survey Checklist (See DoD 8510.1-M, Table AP2.T12).

4.5.3.2. Reviewing the local threats and vulnerabilities.

4.5.3.3. Testing the system installation and security configuration.

4.5.4. After considering the site certification evidence the local Certifier documents the evidence in the SSAA. The local DAA (wing commander) then signs, verifying that the system is installed and operated according to the SSAA.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

CJCSI 6211.02A, Defense Information System Network and Connected Systems, 22 May 1996

CJCSI 6740.01, Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations, 18 September 1996

Information Technology Management Reform Act (ITMRA) of 1996

DoDD 5200.1, DoD Information Security Program, December 13, 1996

DoDI 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), December 30, 1997

DoDD 5200.28, Security Requirements for Automated Information Systems (AISs), March 21, 1988

DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985 (commonly referred to as the Orange Book)

DoD 5220.22-M, National Industrial Security Program Operating Manual, January 1995

DoD 7740.1-G, Department of Defense ADP Internal Control Guideline, July 1998

DoD 8510.1-M, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual, July 31, 2000

OMB Circular A-130, Management of Federal Information Resources

OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information

JP 1-02, Department of Defense Dictionary of Military and Associated Terms, 23 March 1994 as amended through 7 December 1998

P.L. 100-235, Computer Security Act of 1987

Title 5 U.S.C. Section 552a (Privacy Act)

FIPS Pubs 140-2, Security Requirements for Cryptographic Modules, May 25, 2001

AFI 25-201, Support Agreements Procedures

AFI 31-401, Information Security Program Management

AFI 31-601, Industrial Security Program Management

AFI 31-702, System Security Engineering

AFPD 33-2, Information Protection

AFI 33-112, Computer Systems Management

AFI 33-114, Software Management

AFI 33-115V1, Network Management

AFI 33-115V2, Licensing Network Users and Certifying Network Professionals

AFI 33-118, Radio Frequency Spectrum Management

AFI 33-201, (FOUO) Communications Security (COMSEC)

DELETE AFI 33-204, Information Protection Security Awareness, Training, and Education (SATE) Program

AFI 33-205, Information Protection Metrics and Measurements Program

AFI 33-219, Telecommunications Monitoring and Assessment Program (TMAP)

AFMAN 33-120, Radio Frequency (RF) Spectrum Management

AFMAN 33-223, Identification and Authentication

AFMAN 33-229, Controlled Access Protection (CAP)

AFI 65-201, Management Control

AFDIR 33-303, Compendium of Communications and Information Technology

AFSSI 5020, Remanence Security (will convert to AFMAN 33-224)

AFSSI 5021, Vulnerability and Incident Reporting (will convert to AFMAN 33-225V2)

AFSSI 5024V1, The Certification and Accreditation (C&A) Process

AFSSI 5024V2, The Certifying Official's Handbook

AFSSI 5024V3, The Designated Approving Authority's Handbook

AFSSI 5024V4, Type Accreditation

AFSSI 5027, Network Security Policy

AFSSI 7010, (S) Emission Security Assessment (U) (will convert to AFMAN 33-214V1)

Abbreviations and Acronyms

ACC	Air Combat Command
ADP	Automated Data Processing
AETC	Air Education and Training Command
AFCA	Air Force Communications Agency
AFCERT	Air Force Computer Emergency Response Team
AF-CIO	Air Force Chief Information Officer
AFI	Air Force Instruction
AFIWC	Air Force Information Warfare Center
AFMAN	Air Force Manual
AIA	Air Intelligence Agency
AFMC	Air Force Materiel Command

AFPD Air Force Policy Directive

AFSSI Air Force Systems Security Instruction

DELETE AFSSM Air Force Systems Security Memorandum

ASIM Automated Security Incident Monitoring

BIOS Basic Input/Output System

C2 Class 2 (Controlled Access Protection)(a division and class of DoD 5200.28-STD

C&A Certification and Accreditation

CCB Configuration Control Board

CERT Computer Emergency Response Team

CINC Commander-in-Chief

CIO Chief Information Officer

CJCSI Chairman of the Joint Chiefs of Staff Instruction

COMPUSEC Computer Security

COMSEC Communications Security

CONUS Continental United States

DELETE CSM Computer Systems Manager

CSO Communications and Information Systems Officer

DELETE CSSO Computer System Security Officer

DAA Designated Approving Authority

DAC Discretionary Access Control

DISA Defense Information Systems Agency

DISN Defense Information Systems Network

DITSCAP DoD Information Technology Security Certification and Accreditation Process

DoD Department of Defense

DoDD Department of Defense Directive

DRU Direct Reporting Unit

DSAWG DISN Security Accreditation Working Group

EMSEC Emission Security

FIPS Federal Information Processing Standards

FOA Field Operating Agency

FOUO For Official Use Only

FTP	File Transfer Protocol
IA	Information Assurance
IATO	Interim Approval to Operate
I&A	Identification and Authentication
IEEE	Institute of Electrical and Electronics Engineers
DELETE IP	Information Protection
ISP	Internet Service Provider
ISSO	Information System Security Officer
ITMRA	Information Technology Management Reform Act
JP	Joint Publication
JTA-AF	Joint Technical Architecture-Air Force
MAC	Mandatory Access Control
MAJCOM	Major Command
NATO	North Atlantic Treaty Organization
NCC	Network Control Center
NCSC	National Computer Security Center
NIPRNET	Non-Secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NORAD	North American Aerospace Defense Command
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
OSI	Office of Special Investigation
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Associate
PDA	Personal Digital Assistants
P.L.	Public Law
POC	Point of Contact
RAS	Remote Access Server
SABI	Secret and Below Interoperability
DELETE SAF	Secretary of the Air Force
SAF/AA	Administrative Assistant to the Secretary of the Air Force
DELETE SATE	Security Awareness, Training, and Education

SAP/SAR	Special Access Program/Special Access Required
SFUG	Security Feature User's Guide
SIPRNET	Secret Internet Protocol Router Network
SSAA	System Security Authorization Agreement
SSWG	System Security Working Group
TCNO	Time Compliance Network Order
TFM	Trusted Facility Manual
UCM	Unit COMPUSEC Manager
USMCEB	United States Military Communications-Electronic Board
WLAN	Wireless Local Area Network
WM	Workgroup Manager
WWW	World Wide Web
DELETE Y2K	Year 2000

Terms

Accountability 1. Property that allows the ability to identify, verify, and trace system entities as well as changes in their status. Accountability is considered to include authenticity and non-repudiation. 2. (DoD) The obligation imposed by law or lawful order or regulation on an officer or other person for keeping accurate records of property, documents, or funds. The person having this obligation may or may not have actual possession of the property, documents, or funds. Accountability is concerned primarily with records while responsibility is concerned primarily with custody, care, and safekeeping. (JP 1-02)

Accreditation 1. Formal declaration by the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards and controls. 2. (DoD) In computer modeling and simulation, an official determination that a model or simulation is acceptable for a specific purpose. (JP 1-02)

Authenticity Measure of the confidence that the security features and architecture of an information system accurately mediate and enforce the system security policy.

Category A grouping of classified or sensitive information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have access approval (e.g., formal access approval). Examples include proprietary, FOUO, Privacy Act, North Atlantic Treaty Organization (NATO), and compartmented information.

Certification Comprehensive evaluation of the technical and non-technical security features and countermeasures of an information system to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Certifier Individual responsible for making a technical judgment of the information systems compliance with stated security requirements and requesting approval to operate from the DAA.

Communications and Information Systems Officer (CSO) At base level, the commander of the communications unit responsible for carrying out communications and information systems responsibilities. At MAJCOM, the person designated by the MAJCOM/CC responsible for overall management of communications and information systems budgeted and funded by that command. When no other office is formally designated as chief information officer (CIO), the CSO ensures compliance with the mandates of the Information Technology Management Reform Act (ITMRA) of 1996.

Computer-Based Security Security for the information system is provided through the use of automated security features.

DELETE Computer Systems Manager (CSM) Official with supervisory or management responsibility for an organization, activity, or functional area that owns or operates an information system. They are operationally and administratively responsible for the mission that the information system supports. They are responsible for the security-related functions within their office or facilities. (NOTE: This is not an appointed position. For office automation systems, the office chief or manager is normally the CSM.)

DELETE Computer Systems Security Officer (CSSO) Official who manages the COMPUSEC program for an information system assigned to him or her by the CSM; including monitoring information system activities, and ensuring that the information system is operated, maintained, and disposed of according to security policies and practices.

Confidentiality The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls Prescribed actions taken to maintain the appropriate level of protection for information systems. Controls may validate security activities, detect security incidents and non-conformance, correct deficient security countermeasures, measure the assurance of information system activities, or report incidents. (NOTE: There are two divisions of control: management [policy, objectives, and criteria class] and internal [security requirements, mechanisms, and rules]. DoD 7740.1-G, *Department of Defense ADP Internal Control* Guideline, July 1998, outlines internal controls for information systems.)

Countermeasures 1. The sum of a safeguard and its associated controls. 2. (DoD) That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 1-02)

Designated Approving Authority (DAA) Official with the authority to formally assume responsibility for operating an information system or network within a specified environment.

Formal Access Approval Documented approval by a data owner to allow access to a particular category of information.

Information 1. Data derived from observing phenomena and the instructions required to convert that data into meaningful information. (NOTE: Includes: operating system information such as system parameter settings, password files, audit data, etc.) 2. (DoD) Facts, data, or instructions in any medium or form. (JP 1-02) 3. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

Information System 1. Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. (NOTE: This includes automated information systems.) 2. (DoD) The

entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02)

Information Systems Security Officer (ISSO) Official who manages the COMPUSEC program for an information system assigned to him or her by the UCM; including monitoring information system activities, and ensuring that the information system is operated, maintained, and disposed of according to security policies and practices.

Integrity Property that allows the preservation of known unaltered states between baseline certifications and allows information, access, and processing services to function according to specified expectations. It is composed of data and system integrity.

Level of Protection Established safeguards with controls to counter threats and vulnerabilities based on the security requirements. Assures availability, integrity, and confidentiality of the information system.

Nonrepudiation Method by which the sender of data is provided proof of delivery and the recipient is assured of the sender's identity so that neither can deny having processed the data.

Periods Processing Processing of various levels of classified and unclassified information at distinctly different times. (NOTE: Under periods processing, the information system [operating in dedicated security mode] is purged of all information from one processing period before transitioning to the next when there are different users with different authorizations.)

Safeguards Protective measures and controls prescribed to meet the security requirements of an information system. (NOTE: Safeguards include security features and management constraints from the various security disciplines [i.e., administrative, procedural, physical, personnel, communications, emanations, and computer security] used in concert to provide the requisite level of protection.)

Security Feature A hardware-, firmware-, or software-controlled access protection to meet the security requirements of I&A; mandatory access control (MAC); discretionary access control (DAC); object reuse; or audit. Security features are a subset of information system security safeguards.

Sensitive Information Information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. Section 552a (Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept secret in the interest of national defense or foreign policy. (NOTE: Systems that are not national security systems, but contain sensitive information are subject to be protected in accordance with the requirements of the Computer Security Act of 1987 [P.L. 100-235].)

Site Certification Provides assurance that the operational location has implemented the required security measures. This evaluation ensures that the integration and operation of the system is in accordance with the SSAA and a review of the local environment (threats/vulnerabilities).

Stand-Alone System An information system physically and electronically isolated from all other systems and intended to be used by one user at a time, with no data belonging to other users remaining on the system (e.g., a PC with removable storage media such as a floppy disk).

Standard System Two or more substantively similar information systems developed for the purpose of fielding multiple copies in support of a mission, within or across MAJCOM or service lines, or DoD-wide.

System Integrity The attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System Security Policy Set of laws, rules, and practices that regulate how sensitive and classified information is managed, protected, and distributed by an information system. (NOTE: It interprets regulatory [e.g., DoDD 5200.28, AFPD 33-2, AFI 33-202, etc.] and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks, regardless of their sensitivity, criticality, or life-cycle phase, will have a system security policy.)

Tampering Unauthorized modification that alters the proper functioning of information system security equipment.

Threat Current and perceived capability, intention, or attack directed to cause denial of service, corruption, compromise, fraud, waste, or abuse to a system.

User Person or process accessing an information system by direct connections (e.g., via terminals) or indirect connections.

Vulnerability 1. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited. 2. (DoD) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (JP 1-02) 3. (DoD) The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. (JP 1-02)

Workgroup Manager (WM) A duty supporting a functional community (e.g., workcenters, flights, squadrons, or organizations) and is the first line of help customers contact to resolve problems.

Attachment 2

DOD INFORMATION TECHNOLOGY SECURITY CERTIFICATION AND ACCREDITATION PROCESS (DITSCAP) TASKS

Table A2.1. DITSCAP Tasks.

Tasks	DoD 8510.1-M Para #	Output/Product
Phase 1: Definition	Chapter 3	
Preparation	C3.3.2.	
1-1. Review documentation	C3.4.1.	**None**
Registration	C3.3.3.	
1-2. Prepare Mission Description and System Identification	C3.4.2.	**SSAA, Section 1**
1-3. Register System	C3.4.3.	**None**
1-4. Prepare Environment & Threat Description	C3.4.4.	**SSAA, Section 2**
1-5. Determine System Security Requirements	C3.4.5.	**SSAA, Section 4**
1-6. Prepare System Security Architecture Description	C3.4.6	**SSAA, Section 3**
1-7. Identify Organization & Resources	C3.4.7	**SSAA, Section 5**
1-8. Tailor DITSCAP/Prepare DITSCAP Plan	C3.4.8.	**SSAA, Section 6**
1-9. Draft the SSAA	C3.4.9	**Completed draft SSAA Document**
Negotiation	C3.3.4.	
1-10. Conduct Certification Requirements Review	C3.4.10.	**None**
1-11. Establish Agreement on Level of Effort and Schedule	C3.4.11.	**None**
1-12. Approve Phase 1 SSAA	C3.4.12.	**Approved SSAA**
Phase II: Verification	Chapter 4	
SSAA Refinement	C4.2.1.	**If necessary, update SSAA**
Systems Integration and Development	C4.2.2.	**None**
Initial Certification Analysis	C4.2.3.	
2-1. System Architecture Analysis	C4.3.2.	**Minimal Security Activity Checklist and Summary Report**

Tasks	DoD 8510.1-M Para #	Output/Product
2-2. Software, Hardware and Firmware Design Analysis	C4.3.3.	**Minimal Security Activity Checklist and Summary Report**
2-3. Network Connection Rule Compliance	C4.3.4.	**Minimal Security Activity Checklist and Summary Report**
2-4. Integrity Analysis of Integrated Products	C4.3.5.	**Minimal Security Activity Checklist and Summary Report**
2-5. Life Cycle Management Analysis	C4.3.6.	**Minimal Security Activity Checklist and Summary Report**
2-6. Security Requirements Validation Procedures	C4.3.7.	**Customized Minimum Security Checklist, Test Plans and Procedures**
2-7. Vulnerability Assessment	C4.3.8.	**Minimal Security Activity Checklist and Vulnerability Assessment Report**
Phase III: Validation	Chapter 5	
SSAA Refinement	C5.2.1.	**If necessary, update SSAA**
Certification Evaluation of Integrated System	C5.2.2	
3-1. Security Test & Evaluation (ST&E)	C5.3.2.	**Minimal Security Activity Checklist and Summary Report**
3-2. Pentration Testing	C5.3.3.	**Minimal Security Activity Checklist and Summary Report**
3-3. TEMPEST and RED-BLACK Verification	C5.3.4.	**Minimal Security Activity Checklist and Summary Report**
3-4. COMSEC Compliance Evaluation	C5.3.5.	**Minimal Security Activity Checklist and Summary Report**
3-5. System Management Analysis	C5.3.6.	**Minimal Security Activity Checklist and Summary Report**
3-6. Site Accreditation Evaluation	C5.3.7.	**Minimal Security Activity Checklist and Summary Report**
3-7. Contingency Plan Evaluation	C5.3.8.	**Minimal Security Activity Checklist and Summary Report**
3-8. Risk Management Review	C5.3.9.	**Minimal Security Activity Checklist and Summary Report**
Recommendation to DAA	C5.2.3.	**Certifier's Recommendation**
Senior Level SSAA Review	Note 1	**Network Risk Assessment Report**
DAA Accreditation Decision (Note 2)	C5.2.4.	**DAA's Accreditation Letter**
Phase IV: Post-accreditation	Chapter 6	
System and Security Operation	C6.2.1.	

Tasks	DoD 8510.1-M Para #	Output/Product
4-1. SSAA Maintenance	C6.3.2.	**Revised SSAA.**
4-2. Physical, Personnel and Management Control Review	C6.3.3.	**Minimal Security Activity Checklist and Summary Report**
4-3. TEMPEST Evaluation	C6.3.4.	**Summary Report**
4-4. COMSEC Compliance Evaluation	C6.3.5.	**Summary Report**
4-5. Contingency Plan Maintenance	C6.3.6.	**Minimal Security Activity Checklist and Summary Report**
4-6. Configuration Management	C6.3.7.	**Summary Report**
4-7. Risk Management Review	C6.3.8.	**Minimal Security Activity Checklist and Summary Report**
Compliance Validation	C6.2.2.	
4-8. Compliance Validation	C6.3.9.	**Minimal Security Activity Checklist and Summary Report**

NOTES:

1. Systems that do not require a Certificate of Networthiness or Certificate to Operate process still require a Network Risk Assessment performed on them. Stand-alone systems do not require a Network Risk Assessment.

2. DAA's decision to accredit is based on both the Certifier’s recommendation and the Certificate of Networthiness recommendation

Attachment 3

EXAMPLE OF PDA USAGE STATEMENT

MEMORANDUM FOR

FROM: _____ Date: _____

(Rank, Name, Office Symbol)

Subject: Agreement to Use DAA-Approved Privately Owned Personal Digital Assistants (PDA) on the Air Force Enterprise Network

1. My signature below indicates I understand that my privately owned PDA, which is a similar type PDA to the approved government PDAs, has been approved for use by the DAA of the system I am connecting

to. In addition to the requirements in AFI 33-202, *Computer Security*, I agree to all the terms, actions, and conditions contained in this letter.

2. I will:

a. Register my PDA with my local equipment custodian for local accountability.

b. Maintain a password on my PDA according to the system security policy.

c. Only use my PDA to process unclassified, non-Privacy Act information.

d. Maintain the same anti-virus software, security standards, and other operational requirements as the government issued PDAs and pay for what is required.

e. Not connect or subscribe to commercial Internet service provider for official E-mail services.

f. Not synchronize information across the Air Force network using a wireless connection.

g. Physically disable any built-in wireless connectivity capability, including infrared.

h. Surrender my PDA (with no reimbursement) if classified information contaminates my PDA.

i. Report any software abnormalities to the ISSO.

j. Not load any software on my PDA without prior authorization.

k. Submit my personal PDA, prior to leaving my current duty assignment, for removal of all sensitive information.

l. Only connect my PDA to the network or system approved by the DAA.

m. Consent to monitoring of my PDA, since it is connected to a system that is subject to being monitoring.

3. I understand my PDA is subject to being audited at anytime to determine if my PDA contains Privacy Act or classified information.

4. I understand that the process for sanitizing sensitive and classified information from my PDA may result in its destruction and I waive any and all claims for reimbursement for any damage or destruction.

5. I understand the Help Desk will assist me with all PC-related problems but repair of my PDA is my responsibility.

6. I understand that if at any time I fail to meet the conditions stated above, I will be required to remove my PDA from connection within the AF protected enclave and submit it for data sanitization.

7. I understand the Air Force does not assume any liability for my PDA, regardless of circumstance. I understand that all data entered on my PDA while performing government business becomes the property of the U.S. Government.

8. Device information:

a. Make & Model: _____

b. Serial number: _____

c. Operating system: _____

d. Installed software: _____

_____

_____

9. I can be contacted at _____.

(phone number and office symbol)

Signature: _____

Signature Block: _____

File:

1 - Maintain original copy with the ISSO

2 - Provide one copy to the individual